

Management Software

AT-S100

User's Guide

For use with the AT-9000/28 and AT-9000/28SP
Managed Layer 2 GE ecoSwitches

Version 1.0.3

Copyright 2009 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Preface	11
Document Conventions	12
Where to Find Web-based Guides	13
Contacting Allied Telesis	14
Online Support	14
Email and Telephone Support.....	14
Warranty.....	14
Returning Products	14
Sales or Corporate Information	14
Management Software Updates.....	14
Chapter 1: Getting Started with the Command Line Interface	15
Introducing the Command Modes	16
Privileged Executive Command Mode	18
Configuration Terminal Mode.....	19
Interface Configuration Command Mode	20
VLAN Configuration Command Mode.....	21
Line Mode Commands	22
Starting the Command Line Interface	23
Formatting Commands	24
Command Line Interface Features.....	24
Command Formatting Conventions	24
Specifying an Interface.....	24
Command Line Syntax Conventions.....	25
Chapter 2: Configuring the AT-S100 Software	27
Setting the Switch.....	28
Assigning an IP Address	28
Setting DHCP.....	29
Setting a Gateway Address.....	29
Setting the Network Time.....	29
Increasing Frame Size (Jumbo Frames).....	31
Saving the Configuration.....	31
Adding a User Name and Password	31
Displaying and Setting MAC Addresses	32
Rebooting the Switch	35
Resetting Switch to Factory Default Values	35
Upgrading or Downgrading Software	35
Uploading an Image File	37
Displaying and Saving Configuration Files.....	38
Copying Configuration Files.....	39
Uploading and Downloading Configuration Files	39
Creating VLANs	40
Setting the Ports	43
Displaying Port Ethernet Statistics	43
Setting Port Mirroring	43

Setting Port Speed and Duplex Mode	44
Enabling and Disabling Ports	45
Setting MDI and MDIX.....	45
Setting Port Security.....	46
Creating Static Trunks	49
Enabling Backpressure.....	50
Enabling Flow Control	50
Preventing Broadcast Storms.....	51
Configuring Protocols.....	53
Setting GVRP	53
Enabling IGMP Snooping	55
Setting the Link Access Control Protocol (LACP).....	56
Setting 802.1x Port Authentication	56
Configuring RADIUS Authentication.....	58
Setting Simple Network Management Protocol (SNMP)	59
Setting the Secure Shell	62
Setting STP and RSTP	62
Configuring 802.1p Class of Service	67

Section I: Command Modes69

Chapter 3: Privileged Executive Mode Commands	71
CLEAR MAC ADDRESS-TABLE DYNAMIC.....	73
CLEAR MAC ADDRESS-TABLE MULTICAST	75
CLEAR MAC ADDRESS-TABLE STATIC	77
CONFIGURE TERMINAL	79
COPY	81
COPY A.B.C.D	82
COPY DEFAULT.CFG	84
CP	86
DOWNLOAD TFTP	87
EXIT	88
LOGOUT	89
SHOW INTERFACE	90
SHOW MAC ADDRESS-TABLE	92
SHOW MAC ADDRESS-TABLE AGEING-TIME	94
SHOW MAC ADDRESS-TABLE DYNAMIC	96
SHOW MAC ADDRESS-TABLE INTERFACE.....	98
SHOW MAC ADDRESS-TABLE STATIC	100
SHOW MAC ADDRESS-TABLE VLAN.....	102
SHOW RUNNING-CONFIG INTERFACE.....	104
SHOW SPANNING-TREE	106
SHOW STATIC-CHANNEL-GROUP	109
SHOW USER-PRIORITY	110
SYSTEM FACTORY-RESET	111
SYSTEM REBOOT	112
UPLOAD TFTP	113
Chapter 4: Configuration Terminal Mode Commands	115
CLOCK SUMMER-TIME RECURRING	117
CLOCK TIMEZONE	119
CRYPTO KEY GENERATE USERKEY	121
DOT1X SYSTEM-AUTH-CTRL.....	123
ENABLE PASSWORD	124
ENABLE SECRET	125

EXIT.....	126
HELP	127
HOSTNAME	128
INTERFACE	129
IP IGMP SNOOPING.....	131
IP ROUTE.....	132
IP SSH RSA KEYPAIR-NAME	133
IP SSH VERSION.....	134
LINE CONSOLE	135
LINE VTY.....	136
MAC ADDRESS-TABLE AGEING-TIME	138
MAC ADDRESS-TABLE STATIC DISCARD.....	139
MAC ADDRESS-TABLE STATIC FORWARD	141
MLS QOS	143
NTP AUTHENTICATE.....	145
NTP AUTHENTICATION-KEY	146
NTP SERVER.....	148
NTP TRUSTED-KEY	150
SHOW LIST	151
SHOW RUNNING-CONFIG	153
SHOW RUNNING-CONFIG COMMUNITY-LIST	158
SHOW RUNNING-CONFIG INTERFACE	160
USERNAME	162
Chapter 5: Interface Configuration Mode Commands	163
CHANNEL-GROUP	165
DOT1X PORT-CONTROL.....	166
EXIT.....	167
FLOW CONTROL BACKPRESSURE	168
FLOW CONTROL RECEIVE.....	169
FLOW CONTROL SEND.....	170
IP ADDRESS.....	171
IP ADDRESS DHCP.....	173
LACP SYSTEM-PRIORITY	174
MDIX.....	175
MIRROR INTERFACE DIRECTION.....	176
MTU.....	178
SHOW RUNNING-CONFIG INTERFACE	179
SHUTDOWN	181
SPEED	182
STATIC-CHANNEL-GROUP	184
STORM-CONTROL.....	185
SWITCHPORT ACCESS VLAN	187
SWITCHPORT MODE TRUNK	188
SWITCHPORT TRUNK ALLOWED VLAN	190
TRAFFIC-CLASS-TABLE USER-PRIORITY NUM-TRAFFIC-CLASSES	192
USER-PRIORITY	193

Section II: Advanced Configuration 195

Chapter 6: 802.1x Access Control Commands	197
DOT1X PORT-CONTROL.....	198
DOT1X SYSTEM-AUTH-CTRL	199
LOGIN REMOTELOCAL	200
RADIUS-SERVER HOST	201

RADIUS-SERVER KEY	202
SHOW DOT1X	203
SHOW DOT1X ALL	204
SHOW DOT1X INTERFACE	207
SHOW DOT1X STATISTICS INTERFACE	209
Chapter 7: GVRP Commands	211
SET GVRP	212
SET GVRP APPLICANT	213
SET GVRP DYNAMIC-VLAN-CREATION	214
SET GVRP REGISTRATION	215
SET GVRP TIMER	217
Chapter 8: Port Security Commands	219
SWITCHPORT PORT-SECURITY MAC-ADDRESS	220
SWITCHPORT PORT-SECURITY MAXIMUM	222
SWITCHPORT PORT-SECURITY MODE	223
SWITCHPORT PORT-SECURITY VIOLATION	225
Chapter 9: Simple Network Management Protocol (SNMP) Commands	227
SNMP-SERVER COMMUNITY	228
SNMP-SERVER CONTACT	230
SNMP-SERVER ENABLE	232
SNMP-SERVER GROUP	233
SNMP-SERVER HOST	235
SNMP-SERVER USER	237
SNMP-SERVER USER REMOTE	239
SNMP-SERVER VIEW	241
Chapter 10: Spanning Tree Protocol (STP) Commands	243
SHOW SPANNING-TREE	244
SPANNING-TREE ENABLE FORWARD	247
SPANNING-TREE FORWARD-TIME	249
SPANNING-TREE HELLO-TIME	250
SPANNING-TREE MAX-AGE	251
SPANNING-TREE MODE	252
SPANNING-TREE PORTFAST BPDU-FILTER DEFAULT	253
SPANNING-TREE PORTFAST BPDU-GUARD DEFAULT	254
SPANNING-TREE PRIORITY	255
Chapter 11: Virtual Local Area Networks (VLAN) Commands	257
SHOW VLAN ALL	258
SHOW VLAN BRIEF	260
SHOW VLAN DYNAMIC	262
SHOW VLAN STATIC	263
SWITCHPORT TRUNK ALLOWED VLAN	265
VLAN	267
VLAN ACCESS-MAP	268
VLAN DATABASE	269
Index	271

Figures

Figure 1: AT-S100 Command Modes	17
Figure 2: Command Line Login Screen	23
Figure 3: SHOW MAC ADDRESS-TABLE Command	93
Figure 4: SHOW MAC ADDRESS-TABLE AGING-TIME	94
Figure 5: SHOW MAC ADDRESS-TABLE DYNAMIC Command	97
Figure 6: SHOW MAC ADDRESS-TABLE INTERFACE Command	99
Figure 7: SHOW MAC ADDRESS-TABLE STATIC	101
Figure 8: SHOW MAC ADDRESS-TABLE VLAN Command	103
Figure 9: SHOW RUNNING-CONFIG INTERFACE Port Example	104
Figure 10: SHOW RUNNING-CONFIG INTERFACE VLAN Example	105
Figure 11: SHOW SPANNING-TREE Command, page 1	107
Figure 12: SHOW SPANNING-TREE Command, page 2	107
Figure 13: SHOW STATIC-CHANNEL-GROUP	109
Figure 14: SHOW LIST Command	152
Figure 15: SHOW RUNNING-CONFIG Command, page 1	154
Figure 16: SHOW RUNNING-CONFIG Command, page 2	155
Figure 17: SHOW RUNNING-CONFIG Command, page 3	156
Figure 18: SHOW RUNNING-CONFIG Command, page 4	157
Figure 19: SHOW RUNNING-CONFIG INTERFACE Port Example	160
Figure 20: SHOW RUNNING-CONFIG INTERFACE VLAN Example	161
Figure 21: SHOW RUNNING-CONFIG INTERFACE Port Example	179
Figure 22: SHOW RUNNING-CONFIG INTERFACE VLAN Example	180
Figure 23: SHOW DOT1X Command	203
Figure 24: SHOW DOT1X ALL Command	204
Figure 25: SHOW DOT1X INTERFACE Command	207
Figure 26: SHOW DOT1X INTERFACE Command	209
Figure 27: SHOW SPANNING-TREE Command, page 1	245
Figure 28: SHOW SPANNING-TREE Command, page 2	245
Figure 29: SHOW VLAN ALL	258
Figure 30: SHOW VLAN BRIEF	260
Figure 31: SHOW VLAN DYNAMIC	262
Figure 32: SHOW VLAN STATIC	263

Tables

Table 1: Command Modes	17
Table 2: Examples of Privileged Executive Mode Commands	19
Table 3: Examples of Configuration Terminal Mode Commands	20
Table 4: Examples of Interface Configuration Mode Commands	21
Table 5: Examples of VLAN Mode Commands	22
Table 6: Command Line Syntax Conventions	25
Table 7: SHOW DOT1X Parameter Description	205

Preface

The AT-S100 Management Software is the operating system for the AT-9000/28 and AT-9000/28SP Managed Layer 2 GE ecoSwitches. This guide describes the commands included in the management software that you use to control and monitor the operating parameters of both AT-9000 switches.

This Preface contains the following sections:

- ❑ “Document Conventions” on page 12
- ❑ “Where to Find Web-based Guides” on page 13
- ❑ “Contacting Allied Telesis” on page 14

Document Conventions

This document uses the following conventions:

Note

Notes provide additional information.



Caution

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.



Warning

Warnings inform you that performing or omitting a specific action may result in bodily injury.

Where to Find Web-based Guides

The installation and user guides for all Allied Telesis products are available in portable document format (PDF) on our web site at **www.alliedtelesis.com**. You can view the documents online or download them onto a local workstation or server.

For details about the features and functions of the AT-9000/28 and AT-9000/28SP switches, see the following installation guide on our web site:

- ❑ *AT-9000 Managed Layer 2 GE ecoSwitch Family Installation Guide*
(part number 613-001100)

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support as well as sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: **www.alliedtelesis.com/support/kb.aspx**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support section of the Allied Telesis web site: **www.alliedtelesis.com**.

Warranty

The AT-9000/28 9000 Series Managed Layer 2 GE ecoSwitch is covered under a Lifetime Warranty (Two Years Fan & Power Supply). For warranty information, go to the Allied Telesis web site at **www.alliedtelesis.com**.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense. For instructions on how to obtain an RMA number, go to the Support section on our web site at **www.alliedtelesis.com/support.rma.aspx**.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site at **www.alliedtelesis.com**.

Management Software Updates

New releases of the management software for our managed products are available from the following Internet sites:

- ☐ Allied Telesis web site: **www.alliedtelesis.com**
- ☐ Allied Telesis FTP server: **<ftp://ftp.alliedtelesis.com>**

If the FTP server prompts you to log on, enter "anonymous" as the user name and your email address as the password.

Chapter 1

Getting Started with the Command Line Interface

This chapter describes the command modes of the AT-S100 command line interface (CLI) and how to access them. This chapter includes the following sections:

- ❑ “Introducing the Command Modes” on page 16
- ❑ “Starting the Command Line Interface” on page 23
- ❑ “Formatting Commands” on page 24

Introducing the Command Modes

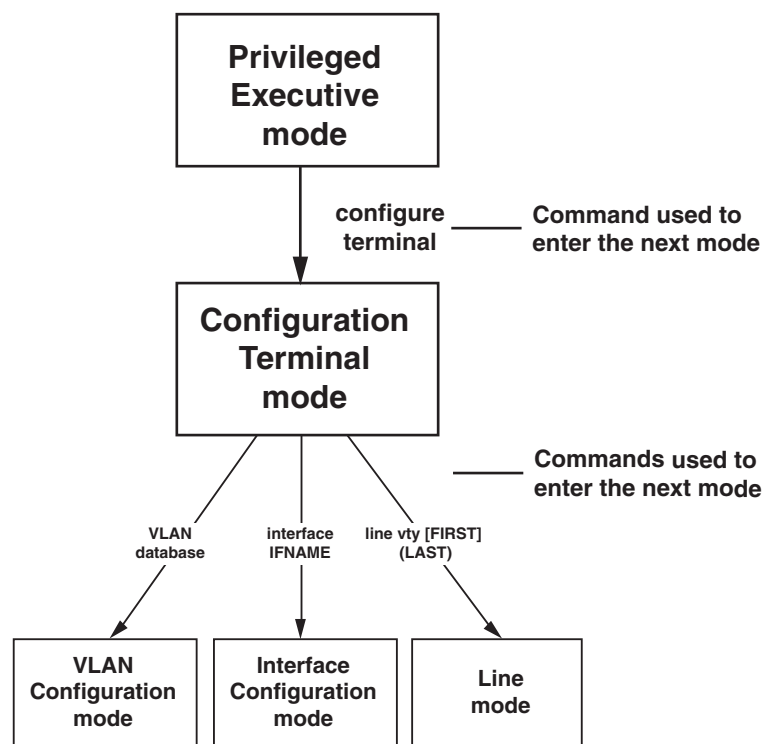
This chapter describes the CLI command modes and how to access the command line interface. There are 5 command modes:

- ❑ Privileged Executive
- ❑ Configuration Terminal
- ❑ VLAN Configuration
- ❑ Interface Configuration
- ❑ Line

In the AT-S100 software, the commands are accessed through a hierarchy of command modes. Each command mode contains a subset of commands that are available within that mode. See Figure 1 on page 17 for an illustration of the command modes.

When you log on to the CLI interface, the default command mode that you access depends on your login id. There are two default login ids that are sent from the factory. The operator login id enables you to display information about the software configuration. With this login, you access the View command mode automatically. The manager login id permits full administrator capabilities. With this login, you access the Privileged Executive mode by default.

You enter a specific command to navigate from one command mode to another. For example, to access the Configuration Terminal mode, enter the CONFIGURE TERMINAL command from the Privileged Executive mode. Once you enter a new command mode, the AT-S100 prompt changes to indicate the new mode.



1221

Figure 1. AT-S100 Command Modes

See Table 1 for information about the commands used to access the modes and their respective prompts.

Table 1. Command Modes

Command Mode	Prompt	Description
Privileged Executive Mode	Switch#	<div><input type="checkbox"/> This is the default command mode for the manager login.</div> <div><input type="checkbox"/> Enter the EXIT or LOGOUT commands to exit the management session.</div>
Configuration Terminal Mode	Switch(config)#	<div><input type="checkbox"/> Use the CONFIGURE command to enter this mode from the Privileged Executive mode.</div> <div><input type="checkbox"/> To return to the Privileged Executive mode, enter the EXIT command.</div>

Table 1. Command Modes (Continued)

Command Mode	Prompt	Description
Interface Configuration	Switch(config-if)#	<ul style="list-style-type: none"> ❑ To access interface 1, enter the following from the Configuration Terminal mode: interface ge1 ❑ Enter the EXIT command to return to the Configuration Terminal mode.
VLAN Configuration	Switch(config-vlan)#	<ul style="list-style-type: none"> ❑ From the Configuration Terminal mode, type the VLAN DATABASE command. ❑ Enter the EXIT command to return to the Configuration Terminal mode.
Line	Switch(config-line)	<ul style="list-style-type: none"> ❑ From the Configuration Terminal mode, type the LINE VTY command. ❑ Enter the EXIT command to return to the Configuration Terminal mode.

In addition, there are commands that allow you to move between the modes. For example, typing the EXIT command when you are in the Interface Configuration mode returns you to the Configuration Terminal mode. From the Privilege Executive mode, the LOGOUT command exits the software.

If you enter a command that is not accessible from a command mode, the software displays a “command not found” message. For example, you can enter the SHOW SNMP command from the Privileged Executive mode, but you cannot enter this command from the VLAN Configuration mode. Within the manual, a command mode is listed for each command.

See the following sections for a description of each command mode:

- ❑ “Privileged Executive Command Mode” on page 18
- ❑ “Configuration Terminal Mode” on page 19
- ❑ “Interface Configuration Command Mode” on page 20
- ❑ “VLAN Configuration Command Mode” on page 21
- ❑ “Line Mode Commands” on page 22

Privileged Executive Command Mode

The Privileged Executive command mode is the default command mode for the manager login. The commands in this mode permit you to perform system level commands such as:

- ❑ rebooting and resetting the system
- ❑ displaying feature configuration and status

- ❑ downloading new image files
- ❑ displaying Ethernet port statistics

The prompt changes to “Switch#” to indicate the Privileged Executive mode.

To access the Configuration Terminal mode from the Privileged Executive mode, enter the CONFIGURE TERMINAL command. To return to the Privileged Executive mode, enter the EXIT command.

See Table 2 for a sample list of commands that can be access from the Privileged Executive command mode. See Chapter 3, “Privileged Executive Mode Commands” on page 71 for detailed information about the commands in this mode.

Table 2. Examples of Privileged Executive Mode Commands

Command	Description
COPY RUN START	Saves the current configuration.
CONFIGURE TERMINAL	Changes the mode to the Configuration Terminal Mode.
COPY	Uploads the configuration file to an image or configuration file.
SHOW INTERFACE	Displays interface configuration and status.
SYSTEM FACTORY- RESET	Resets the AT-S100 software to the factory default settings

Configuration Terminal Mode

The Configuration Terminal mode allows you to configure advanced system features such as:

- ❑ broadcast storm control
- ❑ GVRP
- ❑ IGMP Snooping
- ❑ SNMP
- ❑ STP and RSTP

To access this mode, you must first access the Privileged Executive mode. Then type CONFIGURE TERMINAL to access the Configuration Terminal mode. The prompt changes to “Switch(config)#” to indicate the software has entered the Configuration Terminal mode. To return to the Privilege Executive Mode, enter the EXIT command. To exit the management session, enter the EXIT command again.

See Table 3 for a sample list of commands that can be accessed from the Configuration Terminal mode. For more information about the commands in this mode, see the Chapter 4, “Configuration Terminal Mode Commands” on page 115.

Table 3. Examples of Configuration Terminal Mode Commands

Command	Description
IP-ACCESS-LIST	Creates an access list.
LINE CONSOLE	Sets the console configuration. Accesses the Line mode.
HOSTNAME	Sets the name of the system.
INTERFACE	Accesses the Interface Configuration command mode (you must also specify an interface).
SNMP-SERVER ENABLE	Enables an SNMP agent on the switch.
USERNAME	Sets a system user name and password.

Interface Configuration Command Mode

The Interface Configuration command mode allows you to configure features that pertain to the port and VLAN interfaces such as flow control and duplex mode. To access this mode, you must first access the Privileged Executive and Configuration Terminal modes, depending on your login id.

There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with “ge.” For example, to access port 5 enter the following from the Configuration Terminal mode:

```
interface ge5
```

The prompt changes to “Switch(config-if)#” to indicate the Interface Configuration mode.

To specify a VLAN interface, precede the VLAN ID with “vlan.” For example, to access VLAN 1 (the default VLAN), enter the following from the Configuration Terminal mode:

```
interface vlan1
```

After you have accessed the Interface Configuration mode, the commands you enter apply only to the interface specified in the Configuration Terminal mode. For example, if you enter “interface ge3” in the Configuration Terminal mode, all of the subsequent commands that you enter apply to interface 3 only. To perform interface-specific commands on another interface, do the following:

- ❑ exit the Interface mode by entering the EXIT command
- ❑ specify the new interface in the Configuration Terminal mode
- ❑ re-enter the commands for the new interface

For a sample list of commands that can be accessed from the Interface Configuration command mode, see Table 4. For more detailed information about the commands in the Interface Configuration mode, see Chapter 5, “Interface Configuration Mode Commands” on page 163.

Table 4. Examples of Interface Configuration Mode Commands

Commands	Description
DOT1X MAX-REQ	Sets the maximum number of reauthentication attempts after authentication fails.
FLOWCONTROL ON	Enables flow control and configures the flow control mode for the interface.
IP ADDRESS	Sets an IP address for the switch or specifies that the switch uses a DHCP client to obtain an IP address.
MAC-ADDRESS	Sets the MAC address for a specified interface.
SHUTDOWN	Disables an interface.
SPEED	Sets the speed and duplex mode for an interface.

VLAN Configuration Command Mode

The VLAN Configuration command mode allows you to configure commands that are applied to a specific VLAN interface. For instance, you can assign an IP address to a VLAN interface in this mode.

To access this mode, you must first access the Privileged Executive, and Configuration Terminal modes. From the Configuration Terminal command mode, type the VLAN DATABASE command. The prompt changes to “Switch(config-vlan)#” to indicate the VLAN Configuration mode.

After you have accessed the VLAN Configuration mode, enter commands that apply to a specific VLAN. For a sample list of commands that can be accessed from the VLAN Configuration command mode, see Table 5 on page 22. For more detailed information about the commands in this mode, see Chapter 11, “Virtual Local Area Networks (VLAN) Commands” on page 257.

The default VLAN has a VLAN ID of 1 and it includes all 28 ports. You can configure up to 25 VLANs, with VLAN IDs of between 2 and 4094. However, you cannot configure VLAN 1 as it always remains the default VLAN. In addition, you can display information about VLANs.

Table 5. Examples of VLAN Mode Commands

Commands	Description
SHOW RUNNING-CONFIGURATION SWITCH VLAN	Displays information about VLANs on the switch.
VLAN	Creates a VLAN and enables it.
VLAN NAME	Assigns a name to a VLAN.
VLAN STATE	Sets the operational state of the VLAN.

Line Mode Commands

The Line mode permits you to determine the length of the console lines when creating a Telnet connection and enables password checking on the RADIUS server. Access the Line mode through the Configuration Terminal mode, with the LINE VTY command. The prompt changes to “Switch(config-line)#” to indicate the Line mode.

Once you enter the line mode there is one Line mode command, see “LOGIN REMOTELOCAL” on page 200.

To exit the Line mode and return to the Configuration Terminal mode, use the EXIT command.


Starting the Command Line Interface

To start the command line interface, perform the following procedure:

1. Type the user id and password.

There are two default user ids and passwords. For the system administrator login, the default user id is “manager” and the default password is “friend.”

A command line prompt is displayed in Figure 2.



```
Username:manager
Password:
(none)#
```

Figure 2. Command Line Login Screen

The default switch name is “(none)” and the pound sign (#) prompt indicates the Privileged Executive mode which is the default mode accessed by the manager login.

Formatting Commands

The AT-S100 software command line interface follows the same formatting conventions in all of the command modes. There are command line interface features which apply to the general use of the command line and command syntax conventions which apply when entering the commands. See the following sections.

Command Line Interface Features

The following features are supported in the command line interface:

- ❑ Command history - Use the up and down arrow keys.
- ❑ Context-specific help - Press the question mark key, ?, to display a list of permitted parameters or all of the available commands for a particular command mode. There are two formatting options:
 - command ? - List the keywords or arguments that are required by a particular command. A space between a command and a question mark is required.
 - abbreviated command? - Provides a list of commands that begin with a particular character string. There is no space between the command and the question mark.
- ❑ Keyword abbreviations - Any keyword can be recognized by typing an unambiguous prefix, for example, type “sh” and the software responds with “show.”
- ❑ Tab key - Pressing the Tab key fills in the rest of the keyword automatically. For example, typing “di” and then pressing the Tab key enters “disable” on the command line.

Command Formatting Conventions

The following formatting conventions are used in this manual:

- ❑ screen text font - This font illustrates the format of a command and command examples.
- ❑ ALL CAPITAL LETTERS- All capital letters indicate a command for you to enter.
- ❑ [] - Brackets indicate optional parameters.
- ❑ | - Vertical line separates parameter options for you to choose from.

Specifying an Interface

Both the AT-9000/28 and the AT-9000/28SP switches have 28 ports. Within the command line interface, specify each interface with “ge” and the number of the interface. For example, interface 3 is specified as “ge3.”

Command Line Syntax Conventions

The following table describes the conventions used in the AT-S100 command interface.

Table 6. Command Line Syntax Conventions

Convention	Description	Example
A.B.C.D/M	Indicates an IP address and a subnet mask.	192.68.1.11/24
line	Indicates a line of text that accepts spaces without quotation marks.	Switch 24, San Jose, Building 4
string	Indicates a string of alphanumeric characters, including special characters such as spaces. You must place quotation marks around a value with spaces.	"Switch 24, San Jose, Building 4"
IFNAME or IF_NAME	Indicates an interface name. Specify values ge1 through ge28.	ge3
mask	Indicates a subnet mask.	255.255.240.0
sec	Indicates seconds.	120
min	Indicates minutes.	8
VLANID	Indicates a VLAN instance (including name and VLAN identifier).	vlan3

Chapter 2

Configuring the AT-S100 Software

This chapter provides configuration information about the AT-S100 software. The features are divided into three sections.

This chapter contains the following sections:

- ❑ “Setting the Switch” on page 28
- ❑ “Setting the Ports” on page 43
- ❑ “Configuring Protocols” on page 53

Setting the Switch

The procedures in this section describe how to perform basic switch functions such as assigning an IP address, creating a user name and password, and downloading software. See the following sections:

- ❑ “Assigning an IP Address” on page 28
- ❑ “Setting DHCP” on page 29
- ❑ “Setting a Gateway Address” on page 29
- ❑ “Setting the Network Time” on page 29
- ❑ “Increasing Frame Size (Jumbo Frames)” on page 31
- ❑ “Saving the Configuration” on page 31
- ❑ “Adding a User Name and Password” on page 31
- ❑ “Displaying and Setting MAC Addresses” on page 32
- ❑ “Rebooting the Switch” on page 35
- ❑ “Resetting Switch to Factory Default Values” on page 35
- ❑ “Upgrading or Downgrading Software” on page 35
- ❑ “Uploading an Image File” on page 37
- ❑ “Displaying and Saving Configuration Files” on page 38
- ❑ “Copying Configuration Files” on page 39
- ❑ “Uploading and Downloading Configuration Files” on page 39
- ❑ “Creating VLANs” on page 40

Assigning an IP Address

The IP address for the switch enables you to access the switch through the console port. You must assign an IP address to a VLAN in the Interface Command Mode. You may assign the IP address to the default VLAN which is VLAN 1 or to a VLAN that you have created. For information about how to create a VLAN, see “Creating VLANs” on page 40.

The syntax of the IP address command is:

```
ip address xxx.xxx.xxx.xxx/subnet mask
```

To set the IP address to 192.68.12.8 with a subnet mask of 255.255.255.0 (24 bits) to VLAN 1, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# interface vlan1
```

```
switch(config-if)# ip address 192.68.12.8/24
```

For more information about this command, see “IP ADDRESS” on page 171.

Setting DHCP

The DHCP feature enables the switch to obtain an IP address from the DHCP server. You must assign the DHCP command to the default VLAN, VLAN 1, in the Interface mode. The syntax of the DHCP address command is:

```
ip address dhcp
```

The following example sets the DHCP feature on the switch.

```
switch# configure terminal
switch(config)# interface vlan1
switch(config-if)# ip address dhcp
```

For more information about this command, see “IP ADDRESS DHCP” on page 173.

Setting a Gateway Address

The gateway address consists of an IP address and a subnet mask that you assign to an interface on the switch. The local router uses this information to allow devices that are not on the LAN to communicate with the switch. The syntax of the gate address command, IP ROUTE, is:

```
ip route 0.0.0.0/0 interface
```

To set the gateway address on port 20 to 192.168.1.1 and with a subnet mask of 24, enter the following commands:

```
switch# configure terminal
switch(config)# ip route 192.168.1.1/24 ge20
```

For more information about this command, see “IP ROUTE” on page 132.

Setting the Network Time

The Network Time Protocol (NTP) is used to configure the time on the switch by setting the IP address of an NTP server and setting a key to ensure the proper NTP server has access to the switch. In addition, an NTP server ensures that the time on the switch is set using the Greenwich Mean Standard.

Note

You must have access to an NTP server to use this feature. Allied Telesis does not provide an NTP server.

Setting the NTP Server Address

Setting an NTP server allows the switch to have an official time. The basic syntax of this command is:

```
ntp server xxx.xxx.xxx.xxx
```

To set the IP address of an NTP server to 198.10.1.1, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# ntp server 198.10.1.1
```

For more information about this command, see “NTP SERVER” on page 148.

Turning on NTP Authentication

After you have assigned an NTP server, you can turn on NTP authentication. The basic syntax of this command is:

```
ntp authenticate
```

To turn on NTP authentication, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# ntp authenticate
```

For more information about this command, see “NTP AUTHENTICATE” on page 145.

Configuring an NTP Trusted Key

You may want to configure an NTP Trusted key as a security measure to verify that the NTP server that you have allowed to access your switch is the one you specified.

The basic syntax of this command is:

```
ntp trusted-key <1-xx>
```

To configure an NTP trusted key, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# ntp trusted-key
```

For more information about this command, see “NTP TRUSTED-KEY” on page 150.

Increasing Frame Size (Jumbo Frames)

The jumbo frame command allows an interface on the switch to accept large or jumbo frames which are Ethernet frames with greater than 1,500 bytes of payload (MTU). The syntax of the jumbo frame command is:

```
mtu <64-9216>
```

To allow jumbo frames to be accepted by port 7, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# interface ge7
```

```
switch(config-if)# mtu 1518
```

For more information about this command, see “MTU” on page 178.

Saving the Configuration

To save the current configuration of your switch, use the COPY command. The syntax of this command is:

```
copy running-config startup-config
```

In the following example, the running configuration file is copied to the startup configuration file which is named “startup-config.”

The software displays:

```
Building configuration...
```

```
[OK]
```

For more information about this command, see “COPY” on page 81.

Adding a User Name and Password

To add new users to the switch, you create a user name, determine a privilege level, and assign a password. These tasks are accomplished with the USERNAME command. The syntax of this command is:

```
username WORD privilege <1-15> password LINE <8>
```

Note

By default, the AT-S100 software provides one USERNAME named “manager” with “friend” as the default password. A manager login has permission to perform all of the AT-S100 software commands in all of the command modes.

privilege	Specifies a user privilege level. Enter a value between 1 and 15. Values 1 through 14 provide operator privileges. Value 15 provides an administrator, or manager, privileges.
-----------	--

LINE Specifies a password for an administrator or manager. Enter an alphanumeric value between 1 and 8 characters in length.

The following commands set the user name to “faye,” the privilege to “15,” and the password to “friend:”

```
switch#configure terminal
```

```
switch(config)#username faye privilege 15 password friend
```

For more information about this command, see “USERNAME” on page 162.

Displaying and Setting MAC Addresses

A media access control (MAC) address is a unique number assigned to every network card by the manufacturer. The AT-S100 software keeps track of the MAC addresses of devices that have passed traffic through the switch in a MAC address table. There is an 8K limit of MAC addresses that you can store in the table. As a result, the MAC address table is flushed automatically in time intervals determined by the *ageing time*.

In addition, you can enter a MAC address into the table that cannot be flushed. This type of address is called a *static MAC address*. You may want to assign a static MAC address when you have a closed LAN that is not connected to the Internet.

The following sections explain how to display and set the MAC address table:

- ❑ “Displaying the Full MAC Address Table” on page 32
- ❑ “Displaying the MAC Address Ageing Time” on page 33
- ❑ “Clearing the MAC Address Table” on page 33
- ❑ “Setting the Aging Time” on page 33
- ❑ “Adding a Static MAC Address” on page 34
- ❑ “Removing a Static MAC Address” on page 34

Displaying the Full MAC Address Table

The full MAC address table includes the following information:

- ❑ All static MAC addresses
- ❑ All dynamic MAC addresses
- ❑ MAC addresses assigned to a port
- ❑ MAC addresses assigned to a VLAN

The syntax of this command is:

```
show mac address-table
```


To display the full MAC address table, enter the following command:

```
switch#show mac address-table
```

For more information about this command, including a sample display see “SHOW MAC ADDRESS-TABLE” on page 92.

Displaying the MAC Address Ageing Time

As stated above, the MAC address aging time indicates the time interval when the MAC address table is flushed automatically.

The syntax of this command is:

```
sh mac address-table aging-time
```

To display the MAC address ageing time for the switch, enter the following command:

```
switch#show mac address-table aging-time
```

For more information about this command, including a sample display, see “SHOW MAC ADDRESS-TABLE AGEING-TIME” on page 94.

Clearing the MAC Address Table

You can remove the static, multicast, and static MAC addresses from the MAC address table. The syntax of this command is:

```
clear mac address-table dynamic|static|multicast
```

To remove all of the dynamic commands from the MAC address table enter the following commands:

```
switch# configure terminal
```

```
switch(config)# clear mac address-table dynamic
```

For more information about this command, see “CLEAR MAC ADDRESS-TABLE DYNAMIC” on page 73.

Setting the Aging Time

The MAC address ageing time is set for the switch instead of a port. By default, the ageing time is set to 300 seconds. The syntax of this command is:

```
mac address-table ageing-time (10-1000000)
```

To set the ageing time to 35 seconds, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# mac address-table ageing-time 35
```

For more information about this command, see “MAC ADDRESS-TABLE AGEING-TIME” on page 138.

Adding a Static MAC Address

To add a static address to the MAC address table, specify the MAC address, the assigned port number, and the VLAN ID. The syntax of this command is:

```
mac address-table static (xxxxxxxxxxxx) forward  
interface ge(1-28) vlan(2-4094)
```

To add a static MAC address, 5679AEB04324, on port 15 and VLAN 2 to the MAC address table, enter the following commands:

```
switch# configure terminal  
  
switch(config)# mac address-table static 5679AEB04324  
forward interface ge15 vlan2
```

For more information about this command, see “MAC ADDRESS-TABLE STATIC FORWARD” on page 141.

Removing a Static MAC Address

To remove a static address from the MAC address table you must specify the MAC address, the assigned port number, and the VLAN ID. The syntax of this command is:

```
mac address-table static (xxxxxxxxxxxx) discard  
interface ge(1-28) vlan(2-4094)
```

To remove static MAC address, 5679AEB04322, from port 15 and VLAN 3, enter the following commands:

```
switch# configure terminal  
  
switch(config)# mac address-table static 5679AEB04324  
forward interface ge15 vlan3
```

For more information about this command, see “MAC ADDRESS-TABLE STATIC DISCARD” on page 139.

Rebooting the Switch

To reboot the switch, enter the following command:

```
switch# system reboot
```

When you enter this command the switch temporarily loses power and will the current session is lost. To start a new session on the switch, log in again.

For more information about this command, see “SYSTEM REBOOT” on page 112.

Resetting Switch to Factory Default Values

To reset the AT-S100 software to its factory default values, enter the following command:

```
switch# system factory-reset
```



Warning

This command does not save your current configuration. To save your current configuration, see “COPY DEFAULT.CFG” on page 84.

For more information about this command, see “SYSTEM FACTORY-RESET” on page 111.

Upgrading or Downgrading Software

To upgrade an AT-9000 switch with the latest version of the AT-S100 software, you need to download the software onto your switch with an TFTP server. To obtain the latest version of the AT-S100 software, go to our website, www.alliedtelesis.com and copy it on your PC.

You can use the following procedure to upgrade the AT-S100 software image file to the latest version or downgrade the software to an earlier version. However, it is unlikely that you would want to downgrade the current version of the AT-S100 software to an earlier version.

Note

You do not need to upgrade the bootloader file.

Upgrading or Downgrading the AT-S100 Software with a TFTP Server

Use the following procedure to upgrade or downgrade the AT-S100 software with a TFTP server.

1. Check the current software version installed on your switch, enter the SHOW VERSION command.

See below for a sample output of the SHOW VERSION command:

```
(switch)#show version
```

```
Product ID=ATS100
```

```
Application Version=1.0.3
Application BuildTime=12:47:47
Application BuildDate=Nov 21 2008
Serial Number=
Model=AT-9000/28
Ethaddr=
Baudrate=9600
Uptime= 16:01:02 up 1 min, load average:
0.21, 0.08, 0.02
```

```
HwRev=B
```

2. Assign an IP address and subnet mask to the switch with the IP ADDRESS A.B.C.D/mask command.

The following commands set VLAN 1 with the primary IP address and mask of 192.0.0.1/8.

```
switch#configure terminal
switch(config)#interface vlan1
switch(config-if)#ip address 192.0.0.1/8
```



Caution

Make sure the IP address of the TFTP server is in the same subnet as the IP address of the switch.

3. Save your configuration by entering the following command:

```
switch#copy running-config startup-config
```

4. Use the DOWNLOAD command to download the image file from the TFTP server onto the switch.

The following command uses a TFTP server, with an IP address of 189.11.1.1, to download the “ATS100_ATI_v103.img” file onto the switch:

```
switch#download tftp 189.11.1.1 ATS100_ATI_v103.img
```

The following is displayed:

```
TFTP IP 189.11.1.1, file name
ATS100_ATI_v103.img
```

Erasing 88 Sectors ...

writing to flash ...

5. If you are downgrading the AT-S100 software to an earlier version, the following confirmation message is displayed:

Current version of the image is newer. Download anyway? (y/n)

6. Type “y” to allow the download to proceed.
7. Reboot the switch by entering the following command:

```
(switch)#system reboot
```

Uploading an Image File

The most common reason to upload the image file of the AT-S100 software onto a TFTP server is to make a backup copy of the file. To upload an image file, use the UPLOAD command. You must have the IP address of the TFTP server to set this command.

You do not need to know the name of the image file on the switch to upload it. The filename that you specify in the UPLOAD command indicates the filename on the TFTP server. As a result, you can name it anything you'd like as long as the suffix is “.img.”

Uploading an Image File with a TFTP Server

To upload an image file from the switch onto a TFTP server, use the UPLOAD command. The basic syntax of this command is:

```
upload tftp xxx.xxx.xxx.xxx filename.img
```

Note

Create a dummy file on the TFTP server with the same file name as the file on the switch that you want to upload before you enter the UPLOAD command. If you do not first create the dummy file, you will receive an error message. However, the file will upload successfully.

For example, to upload the image file from the switch onto a TFTP server with an IP address of 192.58.48.10 and a file name of “at100v103.img,” enter the following command:

```
switch# upload tftp 192.58.48.10 at100v103.img
```

The switch displays the following which indicates a successful upload operation:

```
TFTP IP 192.58.48.10, file name at100v103.img
```

For more information about this command, see “UPLOAD TFTP” on page 113.

Displaying and Saving Configuration Files

This section describes how to display and save configuration files. These files have a “.cfg” suffix. See the following sections:

- ❑ “Displaying the Current Configuration” on page 38
- ❑ “Saving the Current Configuration” on page 38

Displaying the Current Configuration

There are several ways to display the current configuration of the switch. You can display the full running configuration of the switch, the running configuration for a port, and the running configuration for a VLAN ID.

The syntax of this command is:

```
show running-config interface ge(1-28) | VLANID
```

To display the full running configuration, enter the following command in any command mode:

```
switch# show running-config
```

In addition, you can display the running configuration for an interface such as a port or a VLAN. To display the running configuration for port 4, enter the following command in any command mode:

```
switch# show running-config interface ge4
```

To display the status of the current running configuration of a switch for VLAN 2, enter the following command:

```
switch#show running-config interface vlan2
```

For more information about this command including a sample display, see “SHOW RUNNING-CONFIG” on page 153.

Saving the Current Configuration

The AT-S100 software does not automatically save your changes. As a result, you want to save your changes to the software frequently. To save the current configuration to the startup configuration file, enter the following command:

```
switch# copy running-config startup-config
```

For more information about this command, see “COPY” on page 81.

Copying Configuration Files

You may want to make a copy of a configuration file in order to have a backup copy of the file. This section describes how you can make a copy a configuration file and save it on your switch.

Copying a Configuration File

Use the CP command to make a copy of a configuration file and save it in the current directory on the switch.

The syntax of CP command is:

```
cp sourcefile newfile
```

Note

The CP command does not save your current configuration onto the switch. To save your current configuration, see the COPY command described in the previous section.

In the following example, the running configuration file is copied to the startup configuration file which is named "frank2.cfg:"

```
switch#cp default.cfg frank2.cfg
```

For more information about this command, see "CP" on page 86.

Uploading and Downloading Configuration Files

Once you have made a copy of the configuration file on the switch, you may want to upload it onto a TFTP server to create a backup copy. Or, you can download a configuration file from a TFTP server onto the switch. See the following sections for a description of these procedures.

You may want to upload a configuration file from your switch onto a backup server. Or, you may want to upload a configuration file from your switch to a TFTP server and then download it to other AT-9000 Series switches. You must have the IP address of the TFTP server to set this command.



Caution

Once you have copied a configuration file onto your PC, use the Wordpad application to open a configuration file in Windows. Do not use the Notepad application to open the file because it deletes all line breaks.

Uploading A Configuration File onto a TFTP Server

Use the COPY DEFAULT.CFG command to upload a configuration file from the switch onto an TFTP server.

Enter the following command to upload a configuration file called “frank2.cfg” from the switch onto a TFTP server with an IP address of 192.58.48.1. The file on the TFTP server is called “at100v103.cfg.”

```
switch# copy frank2.cfg 192.58.48.1 at100v103.cfg
```

For more information about this command, see “COPY DEFAULT.CFG” on page 84.

Downloading A Configuration File from an TFTP Server

To download a configuration file from a TFTP sever to the switch, use the COPY A.B.C.D command. You may want to download a configuration file from a backup server onto your switch. You must have the IP address of the TFTP server to set this command.

To download a configuration file from an TFTP Server, do the following:

1. Enter the following command to download a configuration file called “jenny3.cfg” from a TFTP server with an IP address of 192.58.48.1 onto your switch. The new file is called “at100v103.cfg.”

```
switch# copy 192.58.48.1 jenny3.cfg at100v103.cfg
```

The system responds with the following message:

```
% operation completed.
```

2. Reboot the switch to make the new configuration file the active configuration file. Enter:

```
switch# system reboot
```

3. Log onto the switch with the username of “manager” and the password “friend.”

For more information about this command, see “COPY A.B.C.D” on page 82.

Creating VLANs

A VLAN is a group of ports on an Ethernet switch that form a logical Ethernet segment. The ports of a VLAN form an independent traffic domain where the traffic generated by the nodes of a VLAN remains within the VLAN.

With VLANs, you can segment your network through the switch’s AT-S100 Management Software and group nodes with related functions into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you could create separate VLANs for the different departments in your company, such as one for the sales department and another for the accounting department.

A port-based VLAN is a group of ports on a Gigabit Ethernet Switch that form a logical Ethernet segment. Each port of a port-based VLAN can belong to only one VLAN at a time.

You need to specify which ports will be members of the VLAN. In the case of a tagged VLAN, it is usually a combination of both untagged ports and tagged ports. You specify which ports are tagged and which are untagged when you create the VLAN.

An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs simultaneously.

Creating a VLAN

Use the VLAN command to create a VLAN and enable it. The syntax of this command is:

```
vlan <2-4094> name NAME state enable|disable
```

The following commands create VLAN 4 with a name of “Eng2” and enables it:

```
switch# configure terminal
switch(config)# vlan database
switch(config-vlan)# vlan 2 name Eng2 state enable
```

For more information about this command, see “VLAN” on page 267.

Adding Untagged Ports to a VLAN

To add untagged ports to a VLAN, you must specify a VLAN that you have created already. Also, you must specify a port in the Interface mode. The syntax of this command is:

```
switchport access vlan VLANID <2-4094>
```

The following commands assign VLAN 2 to port 8:

```
switch#configure terminal
switch(config)#interface ge8
switch(config-if)#switchport access vlan 2
```

For more information about this command, see “SWITCHPORT ACCESS VLAN” on page 187.

Adding Tagged Ports to a VLAN

To add tagged ports to a VLAN, you must specify a VLAN that you have created already. You must specify a port in the Interface mode. The syntax of this command is:

```
switchport trunk allowed vlan add|remove VLANID
```

The following commands add VLAN 6, to the member set of port 12:

```
switch#configure terminal
```

```
switch(config)#interface ge12
```

```
switch(config-if)#switchport mode trunk
```

```
switch(config-if)#switchport trunk allowed vlan add 6
```

For more information about this command, see “SWITCHPORT TRUNK ALLOWED VLAN” on page 190.

Setting the Ports

See the following sections:

- ❑ “Displaying Port Ethernet Statistics” on page 43
- ❑ “Setting Port Mirroring” on page 43
- ❑ “Setting Port Speed and Duplex Mode” on page 44
- ❑ “Enabling and Disabling Ports” on page 45
- ❑ “Setting MDI and MDIX” on page 45
- ❑ “Setting Port Security” on page 46
- ❑ “Creating Static Trunks” on page 49
- ❑ “Enabling Backpressure” on page 50
- ❑ “Enabling Flow Control” on page 50
- ❑ “Preventing Broadcast Storms” on page 51

Displaying Port Ethernet Statistics

You may want to display the status of a port as well as configuration information about a port on the switch. The syntax of this command is:

```
show interface ge(1-28)
```

To display the port ethernet statistics for port 17, enter the following command:

```
switch# show interface ge17
```

See “SHOW INTERFACE” on page 90 for a sample display of this command.

Setting Port Mirroring

The port mirror feature allows for the unobtrusive monitoring of ingress or egress traffic on one or more ports on a switch, without impacting network performance or speed. It copies the traffic from a specified port to another port where the traffic can be monitored with a network analyzer.

The port whose traffic is mirrored is called the *source port*. The port where the traffic is copied to is referred to as the *destination port*. The syntax of this command is:

```
mirror interface ge<1-28> direction  
both|receive|transmit
```

To set port mirroring with port 5 as the source port and port 7 as the destination port, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# interface ge5
```

```
switch(config-if)# mirror ge7 direction receive
```

For more information about this command, see “MIRROR INTERFACE DIRECTION” on page 176.

Setting Port Speed and Duplex Mode

A twisted pair port can operate in either half- or full-duplex mode. (Full-duplex mode is the only mode available when a port is operating at 1000 Mbps.) The twisted pair ports are IEEE 802.3u-compliant and Auto-Negotiate the duplex mode setting.

You can disable Auto-Negotiation on one or all of the switch ports so that you can set the duplex mode manually through the AT-S100 Management Software.

Note

In order for a switch port to successfully Auto-Negotiate its duplex mode with a 10 or 100 Mbps end node, the end node should also be configured for Auto-Negotiation. Otherwise, a duplex mode mismatch can occur. A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This results in a mismatch if the end node is operating at a fixed duplex mode of full-duplex.

To avoid this problem when connecting an end node with a fixed duplex mode of full-duplex to a switch port, use the AT-S100 Management Software to disable Auto-Negotiation on the local port and set the port speed and duplex mode manually.

You can set both the port speed and the duplex mode for each port on the switch. The syntax of this command is:

```
speed 1000mfull|100mfull|100mfull|100mhalf|100fx|  
10mfull|10mhalf|auto
```

To set port 28 to 100FX in full-duplex mode, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# interface ge28
```

```
switch(config-if)# speed 100fx
```

For more information about this command, see “SPEED” on page 182.

Enabling and Disabling Ports

To enable or disable a port on the switch, use the SHUTDOWN command. The syntax of this command is:

```
shutdown|no shutdown
```

To enable port 12, enter the following commands:

```
switch# configure terminal
switch(config)# interface ge12
switch(config-if)# shutdown
```

To disable port 19, enter the following commands:

```
switch# configure terminal
switch(config)# interface ge19
switch(config-if)# no shutdown
```

For more information about this command, see “SHUTDOWN” on page 181.

Setting MDI and MDIX

The twisted pair ports on the switch feature auto-MDI and MDIX. This feature, available when a port's speed and duplex mode are set through Auto-Negotiation, configures a switch port to MDI or MDIX automatically, depending on the wiring configuration of the port on the end node. This feature allows you to connect any network device to a port on the switch using a straight-through twisted pair cable.

If Auto-Negotiation is disabled on a port and the speed and duplex mode are set manually, the auto-MDI/MDI-X feature is also disabled and the port's wiring configuration defaults to the MDI-X setting. This setting can be configured with the AT-S100 Management Software.

The syntax of this command is:

```
mdix mdi|mdix
```

To set a port to MDI, enter the following commands:

```
switch# configure terminal
switch(config)# interface ge12
switch(config-if)# mdix mdi
```

To set a port to MDIX, enter the following commands:

```
switch# configure terminal  
switch(config)# interface ge12  
switch(config-if)# mdix mdix
```

For more information about this command, see “MDIX” on page 175.

Setting Port Security

The Port Security feature is based on assigning and limiting MAC addresses learned by a port. You can use the MAC-Address-based Port Security feature to enhance the security of your network by controlling which end nodes can forward frames through the switch, thereby preventing unauthorized individuals from accessing your network. This feature uses a MAC address to determine whether the switch should forward a frame or discard it. The source address is the MAC address of the end node that sent the frame.

There are three levels of port security:

- ☐ Limited Mode
- ☐ Locked Mode
- ☐ Secured Mode

You set port security on a per port basis. Only one security level can be active on a port at a time.

Limited Mode

The Limited security mode allows you to specify the maximum number of dynamic MAC addresses a port can learn. The port forwards only packets of learned source MAC addresses and discards ingress frames with unknown source MAC addresses.

When the Limited security mode is initially activated on a port, all dynamic MAC addresses learned by the port are deleted from the MAC address table. The port then begins to learn new addresses, up to the maximum allowed. After the port has learned its maximum number of addresses, it does not learn any new addresses, even when end nodes are inactive.

A dynamic MAC address learned on a port operating in the Limited security mode never times out from the MAC address table, even when the corresponding end node is inactive.

Static MAC addresses are retained by the port and are not included in the count of maximum dynamic addresses. You can continue to add static MAC addresses to a port operating with this security level, even after the port has already learned its maximum number of dynamic MAC addresses.

Locked Mode

A port set to the Locked mode security level immediately stops learning new dynamic MAC addresses and forwards frames using the dynamic MAC addresses it has already learned and any static MAC addresses assigned to it. Ingress frames with an unknown MAC address are discarded. Dynamic MAC addresses already learned by a port prior to the activation of this security level never time out from the MAC address table, even when the corresponding end nodes are inactive.

You can continue to add new static MAC addresses to a port operating under this security level.

Secured Mode

The Secured Mode security level uses only static MAC addresses assigned to a port to forward frames. Consequently, only those end nodes whose MAC addresses are entered as static addresses are able to forward frames through a port. Dynamic MAC addresses already learned on a port are discarded from the MAC table and no new dynamic addresses are added. Any ingress frames having a source MAC address not entered as a static address on a port are discarded.

After activating this security level, you must enter the static MAC addresses of the end nodes that are to forward frames through the port.

MAC Address Maximum

In addition, you can set the maximum number of MAC addresses that can be learned by a port as well as specific secure MAC addresses that can be learned by a port.

Once the limit of MAC addresses is reached for the port specified, the action taken by the software is determined by the setting of the SWITCHPORT PORT-SECURITY VIOLATION command. There are 3 possible responses to a violation:

- ☐ Protect
- ☐ Restrict
- ☐ Shutdown

Setting the Maximum Number of MAC Addresses

To limit the number of MAC addresses that can be learned by a port, use the SWITCHPORT PORT-SECURITY MAXIMUM command.

The syntax of this command is:

```
switchport port-security maximum <1-320>
```

To set the maximum number of MAC addresses to 140 on port 8, enter the following commands:

```
switch# configure terminal
switch(config)# interface ge8
switch(config-if)#switchport port-security maximum 140
```

For more information about this command, see “” on page 189.

Assigning Secure MAC Addresses

Assigning the predefined MAC addresses that can be learn on a port, allows you to limit the devices that can access the port.

The syntax of this command is:

```
switchport port-security mac address xxxx.xxxx.xxxx
vlan <2-4094>
```

To add a secure predefined mac address of 00A0.0490.10E0 to port 21 which is assigned to VLAN 3, enter the following commands:

```
switch# configure terminal
switch(config)# interface ge21
switch(config-if)#switchport port-security mac address
00A0.0490.10E0 vlan 3
```

For more information about this command, see “” on page 189.

Setting the Port Security Mode

The Port Security Mode determines how a port responds to an undefined MAC address. The syntax of this command is:

```
switchport port-security mode limited|locked|secured
```

To set the port security mode to limited on port 17, enter the following commands:

```
switch# configure terminal
switch(config)# interface ge17
switch(config-if)#switchport port-security mode
limited
```

For more information about this command, see “SWITCHPORT PORT-SECURITY MODE” on page 223.

Setting Port Security Violation

The Port Security Violation Feature determines how the AT-S100 software reacts when the number of port secure MAC addresses reaches the maximum value set in the SWITCHPORT PORT-SECURITY MAXIMUM command (see “Setting the Maximum Number of MAC Addresses” on page 47.)

The syntax of SWITCHPORT PORT-SECURITY VIOLATION command is:

```
switchport port-security violation
protect|restrict|shutdown
```

To set the port security violation mode on port 20 to restrict, enter the following commands:

```
switch# configure terminal
switch(config)# interface ge20
switch(config-if)#switchport port-security violation
restrict
```

For more information about this command, see “SWITCHPORT PORT-SECURITY VIOLATION” on page 225.

Creating Static Trunks

A static port trunk is a group of two to eight ports that function as a single virtual link between the switch and another device. Traffic is distributed across the ports to improve performance and enhance reliability by reducing the reliance on a single physical link.

To configure a static port trunk, you designate the ports of the trunk and the management software groups them together automatically. You can also control how traffic is distributed over the trunk ports.

The syntax of the static trunk command is:

```
static-channel-group<1-8>
```

For example, to assign port 8 to static port trunk 2, enter the following commands:

```
switch# configure terminal
switch(config)# interface ge8
switch(config-if)# static-channel-group2
```

To display the static port trunk assigned to port 12, enter the following commands:

```
switch# configure terminal  
switch(config)# interface ge12  
switch(config-if)# show static-channel-group9
```

For more information about this command, see “STATIC-CHANNEL-GROUP” on page 184.

Enabling Backpressure

To maintain the orderly movement of data between the end nodes, an Ethernet switch may periodically need to signal an end node to stop sending data. This can occur under several circumstances. For example, if two end nodes are operating at different speeds, the switch, while transferring data between the end nodes, might need to instruct the faster end node to stop transmitting data to allow the slower end node to catch up. An example of this would be when a server operating at 100 Mbps is sending data to a workstation operating at only 10 Mbps.

How a switch signals an end node to stop transmitting data differs depending on the speed and duplex mode of the end node and switch port. A twisted pair port operating at 100 Mbps and half-duplex mode stops an end node from transmitting data by forcing a collision. A collision on an Ethernet network occurs when two end nodes attempt to transmit data using the same data link at the same time. A collision causes end nodes to stop sending data. To stop a 100 Mbps, half-duplex end node from transmitting data, the switch forces a collision on the data link, which stops the end node. When the switch is ready to receive data again, the switch stops forcing collisions. This is referred to as back pressure.

The syntax of this command is:

```
flowcontrol backpressure on|off
```

To active the backpressure feature on port 3, enter the following commands:

```
switch# configure terminal  
switch(config)# interface ge3  
switch(config-if)# flowcontrol backpressure on
```

For more information about this command, see “FLOW CONTROL BACKPRESSURE” on page 168.

Enabling Flow Control

Flow control enables connected Ethernet ports (or interfaces) to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot

receive any more traffic, it notifies another port to stop sending traffic until the condition clears. When the local device detects congestion at its end, it notifies the remote device by sending a pause frame. After the remote device receives a pause frame, the remote device stops sending data packets. Flow control prevents the loss of data packets during the congestion period.

The flow control command determines whether flow control is set to *transmit* or *receive* on a port. Flow control is set on a per port basis. The basic command syntax is:

```
flowcontrol send|receive on|off
```

To set the flow control to transmit on port 7, enter the following commands:

```
switch# configure terminal
switch(config)# interface ge7
switch(config-if)# flowcontrol send on
```

For more information about this command, see “FLOW CONTROL SEND” on page 170.

To set the flow control to receive on port 8, enter the following commands:

```
switch# configure terminal
switch(config)# interface ge8
switch(config-if)# flowcontrol receive on
```

For more information about this command, see “FLOW CONTROL RECEIVE” on page 169.

Preventing Broadcast Storms

Flooding techniques are used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on an interface. Forwarding these packets can cause the network to slow down or timeout.

Use the STORM-CONTROL command to specify the rising threshold level for broadcasting, multicast, or destination-lookup-failure traffic. The storm control action occurs when traffic reaches the level specified with the LEVEL parameter. By default, storm control is disabled.

To prevent broadcast storms, enter the following commands:

```
switch# configure terminal
switch(config)# interface ge2
```

```
switch(config-if)#storm-control broadcast level (0.0-100.0)
```

To prevent multicast storms, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# interface ge2
```

```
switch(config-if)# storm-control multicast level (0.0-100.0)
```

To configure for destination-lookup-failure traffic, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# interface ge2
```

```
switch(config-if)# storm-control dlf level (0.0-100.0)
```

For more information about this command, see “STORM-CONTROL” on page 185.

Configuring Protocols

This section describes how to set the protocols that are supported by the AT-S100 Management Software. See the following sections:

- ❑ “Setting GVRP” on page 53
- ❑ “Enabling IGMP Snooping” on page 55
- ❑ “Setting the Link Access Control Protocol (LACP)” on page 56
- ❑ “Setting 802.1x Port Authentication” on page 56
- ❑ “Configuring RADIUS Authentication” on page 58
- ❑ “Setting Simple Network Management Protocol (SNMP)” on page 59
- ❑ “Setting the Secure Shell” on page 62
- ❑ “Setting STP and RSTP” on page 62
- ❑ “Configuring 802.1p Class of Service” on page 67

Setting GVRP

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information. The main purpose of GVRP is to allow switches to automatically discover some of the VLAN information that would otherwise need to be manually configured in each switch. This is helpful in networks where VLANs span more than one switch. Without GVRP, you must manually configure your switches to ensure that the various parts of a VLAN can communicate across the different switches. GVRP, which is an application of the Generic Attribute Registration Protocol (GARP), does this for you automatically.

The AT-S100 Management Software uses GVRP protocol data units (PDUs) to share VLAN information among GVRP-active devices. The PDUs contain the VID numbers of the VLANs on the switch. A PDU contains the VIDs of all the VLANs on the switch, not just the VID of which the transmitting port is a member.

When a switch receives a GVRP PDU on a port, it examines the PDU to determine the VIDs of the VLANs on the device that sent it.

Enabling or Disabling GVRP

By default, the GVRP feature is disabled. The syntax of the command is:

```
set gvrp enable|disable
```

To enable the GVRP feature, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# set gvrp enable
```

To disable the GVRP feature, enter the following commands:

```
switch# configure terminal
switch(config)# set gvrp disable
```

For more information about this command, see “SET GVRP” on page 212.

Setting the GVRP Applicant State

By setting the GVRP applicant state, you permit a port to process GVRP information and transmit PDUs. The GVRP APPLICANT command sets the GID applicant state on a port to active or normal. The syntax of this command is:

```
set gvrp applicant state active|normal ge<1-28>
```

To set the GID applicant on port 5 to an active state enter the following commands:

```
switch#configure terminal
switch(config)#set gvrp applicant state active ge5
```

For more information about this command, see “SET GVRP APPLICANT” on page 213.

Enabling Dynamic VLANs

To enable dynamic VLANs to be created on the switch, use the GVRP DYNAMIC-VLAN-CREATION command. The syntax of this command is:

```
set gvrp dynamic-vlan-creation
```

The following commands allow GVRP VLANs to be created dynamically:

```
switch#configure terminal
switch(config)#set gvrp dynamic-vlan-creation
```

For more information about this command, see “SET GVRP DYNAMIC-VLAN-CREATION” on page 214

Setting GVRP Registration

You can allow manual creation of VLANs (fixed), deregister all existing VLANs with the exception of VLAN 1 (forbidden), and allow dynamic VLAN creation on a per port basis (normal).

The syntax of this command is:

```
set gvrp registration fixed|forbidden|normal ge<1-28>
```

The following commands set GVRP registration to fixed on port 12:

```
switch#configure terminal
```

```
switch(config)#set gvrp registration fixed ge12
```

For more information about this command, see “SET GVRP REGISTRATION” on page 215.

Setting Join and Leave Timers

To set the GARP timers to join or leave a group, use the SET GVRP TIMER command. The syntax of this command is:

```
set gvrp timer join|leave|leaveall <1-65535> ge<1-28>
```

The following commands set the leave timer to 0.5 seconds for all GVRP applications on port 9:

```
switch#configure terminal
```

```
switch(config)#set gvrp timer leave 50 seconds ge9
```

For more information about this command, see “SET GVRP TIMER” on page 217.

Enabling IGMP Snooping

IPv4 routers use IGMP to create lists of nodes that are members of multicast groups. (A multicast group is a group of end nodes that want to receive multicast packets from a multicast application.) The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports. The syntax of this command is:

```
no|ip igmp snooping
```

To enable IGMP, enter the following commands:

```
switch# config t
```

```
switch(config)# ip igmp snooping
```

To disable IGMP, enter the following commands:

```
switch# config t
```

```
switch(config)# no ip igmp snooping
```

Setting the Link Access Control Protocol (LACP)

LACP (Link Aggregation Control Protocol) port trunks perform the same function as static trunks. They increase the bandwidth between network devices by distributing the traffic load over multiple physical links. The advantage of an LACP trunk over a static port trunk is its flexibility. While implementations of static trunking tend to be vendor specific, the implementation of LACP in the AT-S100 Management Software is compliant with the IEEE 802.3ad standard, making it interoperable with equipment from other vendors that also comply with the standard. Therefore, you can create an LACP trunk between an Allied Telesis device and network devices from other manufacturers.

Another advantage is that ports in an LACP trunk can function in a standby mode. This adds redundancy and resiliency to the trunk. If a link in a static trunk goes down, the overall bandwidth of the trunk is reduced until the link is reestablished or another port is added to the trunk. In contrast, an LACP trunk can automatically activate ports in a standby mode when an active link fails so that the maximum possible bandwidth of the trunk is maintained.

The syntax of this command is:

```
channel-group (1-10) mode active|passive
```

To configure LACP on port 12 and channel group 1, enter the following commands:

```
switch# config t
```

```
switch(config)# interf ge12
```

```
switch(config-if)# channel-group 1 mode active
```

To disable LACP on port 7 and channel group 2, enter the following commands:

```
switch# config t
```

```
switch(config)# interf ge7
```

```
switch(config-if)# no channel-group 2 mode passive
```

Setting 802.1x Port Authentication

The AT-S100 Management Software has several different methods for protecting your network and its resources from unauthorized access. One method is 802.1x port-based network access control which uses the RADIUS protocol to control who can send traffic through and receive traffic from a switch port. The switch does not allow an end node to send or receive traffic through a port until the user of the node has been authenticated by a RADIUS server.

The benefit of this type of network security is that you can prevent unauthorized individuals from connecting a computer to a switch port or

using an unattended workstation to access your network resources. Only those users designated as valid network users on the RADIUS server are permitted to use the switch to access the network.

The switch implements the server side of the IEEE 802.1x Port-based and MAC-based Network Access Control. This feature allows only authorized users, or their network devices, access to network resources by establishing criteria for each interface on the switch.

Displaying 802.1x Port Authentication Status

Displaying the status of the 802.1x Port Authentication feature on the switch provides the following information:

- ❑ 802.1x Port Authentication status (enabled or disabled)
- ❑ RADIUS server IP address
- ❑ RADIUS client IP address
- ❑ Next RADIUS message ID

The syntax of this command is:

```
show dot1x
```

To display the status of the 802.1x Port Authentication feature, enter the following command:

```
switch#show dot1x
```

For more information about this command including a display, see “SHOW DOT1X” on page 203.

Setting 802.1x Port Authentication

To set 802.1x Port Authentication with a RADIUS server host of 192.168.1.30 and a shared secret key between the RADIUS server and a client of “Encrypt112,” enter the following commands:

```
switch# configure terminal
switch(config)# dot1x system-auth-ctrl
switch(config)# interface ge12
switch(config-if)# dot1x port-control auto
switch(config-if)# exit
switch(config)# radius-server host 192.168.1.30
switch(config)# radius-server key Encrypt112
```

For more information about the 802.1x commands, see Chapter 6, “802.1x Access Control Commands” on page 197.

Configuring RADIUS Authentication

For those networks managed by just one or two network managers, you might not need any additional accounts. In the case of larger networks that are managed by several network managers, you may want to give each manager his or her own management login account for a switch rather than have them share an account.

This is where authentication protocols such as RADIUS can be useful. RADIUS is an acronym for Remote Authentication Dial In User Services. You can use RADIUS to transfer the task of validating management access from the switch to an authentication protocol server, enabling you to create your own manager accounts.

With RADIUS you can create a series of username and password combinations that define who can manage the switch.

There are three basic functions an authentication protocol provides:

- ☐ Authentication
- ☐ Authorization
- ☐ Accounting

When a network manager logs in to a switch to manage the device, the switch passes the username and password entered by the manager to the authentication protocol server. The server checks to see if the username and password are valid. This is referred to as authentication.

If the combination is valid, the authentication protocol server notifies the switch and the switch completes the login process, allowing the manager to manage the switch.

If the username and password are invalid, the authentication protocol server notifies the switch and the switch cancels the login.

Authorization defines what a manager can do after logging in to a switch.

The final function of an authentication protocol is keeping track of user activity on network devices, referred to as accounting. The AT-S100 Management Software does not support RADIUS accounting as part of manager accounts.

Note

This manual does not explain how to configure a RADIUS server. For instructions, refer to the documentation included with the RADIUS server software.

Setting RADIUS Authentication

To set RADIUS authentication with a RADIUS-server host of 192.168.1.30, a shared secret key of "Encrypt112," and RADIUS password checking turned on, enter the following commands:

```
switch# configure terminal
switch(config)# radius-server host 192.168.1.30 auth-
port 1812
switch(config)# radius-server key Encrypt112
switch(config)# line console 0
switch(config-line)# login remotelocal
```

For more information about the 802.1x commands, see Chapter 6, "802.1x Access Control Commands" on page 197.

Setting Simple Network Management Protocol (SNMP)

You can manage a switch by viewing and changing the management information base (MIB) objects on the device with the Simple Network Management Program (SNMP). The AT-S100 Management Software supports SNMPv1 and SNMPv2c protocols.

To manage a switch using an SNMP application program, you must do the following:

- ☐ Activate SNMP management on the switch. The default setting for SNMP management is disabled.
- ☐ Load the Allied Telesis MIBs for the switch onto your management workstation containing the SNMP application program. The MIBs are available from the Allied Telesis web site at www.alliedtelesis.com.

To manage a switch using SNMP, you need to know the IP address of the switch or of the master switch of an enhanced stack and at least one of the switch's community strings.

Enabling and Disabling SNMP

You enable and disable the SNMP protocol on the switch. The syntax of this command is:

```
no|snmp-server enable
```

To enable the SNMP protocol, enter the following commands:

```
switch# configure terminal
switch(config)# snmp-server enable
```

To disable the SNMP protocol, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# no snmp-server enable
```

For more information about this command, see “SNMP-SERVER ENABLE” on page 232.

Creating an SNMP Contact Name

The SNMP contact name is a person who is to be contacted in case of questions about your SNMP implementation, an email address, or an IP address for the SNMP system. The syntax of this command is:

```
snmp-server contact “John Smith”
```

To create an SNMP contact name of John Smith, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# snmp-server contact “John Smith”
```

For more information about this command, see “SNMP-SERVER CONTACT” on page 230.

Creating SNMP Communities

SNMP Communities have several attributes, including a name and an access mode. A community name must have a name of one to eight alphanumeric characters. Spaces are allowed.

The access mode attribute defines the permissions of a community string. There are two access modes: Read and Read/Write. A community string with an access mode of Read can only be used to view (but not change the MIB objects on a switch). A community string with a Read/Write access can be used to both view the MIB objects and change them.

The AT-S100 Management Software provides two default community strings: public and private. The public string has an access mode of just Read and the private string has an access mode of Read/Write. If you activate SNMP management on the switch, delete or disable the private community string, which is a standard community string in the industry, or change its status from open to closed to prevent unauthorized changes to the switch.

The syntax of this command is:

```
snmp-server community <community name> <ro|rw|view>
```

To create an SNMP community called public with an access level of Read only, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# snmp-server community public ro
```

For more information about this command, see “SNMP-SERVER COMMUNITY” on page 228.

Adding Management and Trap Receiver Addresses

A trap is a signal sent to one or more management workstations by the switch to indicate the occurrence of a particular operating event on the device. There are numerous operating events that can trigger a trap. For instance, resetting the switch or the failure of a cooling fan are two examples of occurrences that cause a switch to send a trap to the management workstations. You can use traps to monitor activities on the switch.

Trap receivers are the devices, typically management workstations or servers, that you want to receive the traps sent by the switch. You specify the trap receivers by their IP addresses. You assign the IP addresses to the community strings.

Each community string can have up to eight trap IP addresses.

It does not matter which community strings you assign your trap receivers. When the switch sends a trap, it looks at all the community strings and sends the trap to all trap receivers on all community strings. This is true even for community strings that have a access mode of only Read.

If you are not interested in receiving traps, then you do not need to enter the IP addresses of trap receivers.

To add a management and trap receiver IP address, enter the following commands:

```
switch# config t
```

```
switch(config)# snmp-server host <ip address> version  
1|2c <community name> traps
```

```
snmp-server host 192.168.1.2 version 1 public
```

```
snmp-server host 192.168.1.2 version 1 trap
```

For more information about all of the SNMP commands, see Chapter 9, “Simple Network Management Protocol (SNMP) Commands” on page 227.

Setting the Secure Shell

Secure management is increasingly important in modern networks, as the ability to easily and effectively manage switches and the requirement for security are two universal requirements. Switches are often remotely managed using remote sessions via the Telnet protocol. This method, however, has a serious security problem—it is only protected by plaintext usernames and passwords which are vulnerable to wiretapping and password guessing.

The Secure Shell (SSH) protocol provides encrypted and strongly authenticated remote login sessions, similar to the Telnet and rlogin protocols, between a host running a Secure Shell server and a machine with a Secure Shell client.

The syntax of this command is:

```
crypto key generate userkey USERNAME rsa <768-32768>
```

To generate a 2048-bit RSA user key for SSH version 2 connections for a user named “mel,” enter the following commands:

```
switch#configure terminal
```

```
switch(config)#crypto key generate userkey mel rsa
2048
```

For more information about this command, see “CRYPTO KEY GENERATE USERKEY” on page 121.

Setting STP and RSTP

The performance of a Ethernet network can be negatively impacted by the formation of a data loop in the network topology. A data loop exists when two or more nodes on a network can transmit data to each other over more than one data path. The problem that data loops pose is that data packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and can significantly reduce network performance.

STP and RSTP prevent data loops from forming by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, these protocols place the extra paths in a standby or blocking mode, leaving only one main active path.

STP and RSTP can also activate a redundant path if the main path goes down. So not only do these protocols guard against multiple links between segments and the risk of broadcast storms, but they can also maintain network connectivity by activating a backup redundant path in case a main link fails.

Where the two protocols differ is in the time each takes to complete the process referred to as *convergence*. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol must determine whether there are redundant paths that must be

blocked to prevent data loops, or activated to maintain communications between the various network segments. This is the process of convergence.

With STP, convergence can take up to a minute to complete in a large network. This can result in the loss of communication between various parts of the network during the convergence process, and the subsequent lost of data packets.

RSTP is much faster. It can complete a convergence in seconds, and so greatly diminish the possible impact the process can have on your network.

Only one spanning tree protocol can be active on the switch at a time. The default is RSTP.

Setting the Spanning Tree Mode

As mentioned above, the default setting for the spanning tree mode is RSTP. To change the current spanning tree mode setting, use the SPANNING-TREE MODE command. The syntax of this command is:

```
spanning-tree mode stp|rstp
```

To set the spanning tree mode to STP, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# spanning-tree mode stp
```

For more information about this command, see “SPANNING-TREE MODE” on page 252.

Displaying Spanning Tree Settings

The spanning tree display includes the following information:

- ☐ Bridge setting
- ☐ Root Path Cost
- ☐ Root Port
- ☐ Bridge Priority
- ☐ Forward Delay time
- ☐ Hello time
- ☐ Maximum Age
- ☐ Root ID

The syntax of this command is:

```
show spanning-tree
```

To display the current spanning tree settings for the STP mode, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# spanning-tree mode stp
```

```
switch(config)# show spanning-tree
```

For more information about this command including a display, see “SHOW SPANNING-TREE” on page 244.

Enabling or Disabling the Spanning Tree Mode

To enable or disable the spanning tree mode on the switch, use the SPANNING-TREE ENABLE FORWARD command. The syntax of this command is:

```
spanning-tree stp|rstp enable forward
```

To enable STP, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# spanning-tree stp enable forward
```

To disable the RSTP on the switch, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# no spanning-tree rstp enable forward
```

For more information about this command, see “SPANNING-TREE ENABLE FORWARD” on page 247.

Setting Spanning-Tree Priority

Use the SPANNING-TREE PRIORITY command to specify the interface priority for the switch. A lower priority value indicates a greater likelihood of becoming a root. The default value is 32,768.

The syntax of this command is:

```
spanning-tree priority (0-61440)
```


The following commands set the spanning-tree priority on the switch to 8,192:

```
switch#configure terminal
```

```
switch(config)#spanning-tree priority 8192
```

For more information about this command, see “SPANNING-TREE PRIORITY” on page 255.

Setting the Max Age

The max-age is the maximum time, in seconds, which a message is considered valid (if a bridge is the root bridge). This setting prevents the frames from looping indefinitely. This value is used by all instances.

The syntax of this command is:

```
spanning-tree max-age (6-40)
```

The following commands set the max-age time for the bridge to 30 seconds:

```
switch#configure terminal
```

```
switch(config)#spanning-tree max-age 30
```

For more information about this command, see “SPANNING-TREE MAX-AGE” on page 251

Setting the Forward Time

Use the SPANNING-TREE FORWARD-TIME command to set the time, after which each interface changes to the learning and forwarding states (if this bridge is the root bridge). This value is measured in seconds and it is used by all instances. The syntax of this command is:

```
spanning-tree forward-time (4-30)
```

The following commands set the forward delay time to 10 seconds:

```
switch#configure terminal
```

```
switch(config)#spanning-tree forward-time 10
```

For more information about this command, see “SPANNING-TREE FORWARD-TIME” on page 249.

Setting the Hello Time

The hello-time is the time, in seconds, after which all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). For this to

occur, the current bridge must be the root bridge. A very low value of this command leads to excessive traffic on the network, while a higher value delays the detection of topology change. This value is used by all instances.

The syntax of this command is:

```
spanning-tree hello-time (1-10)
```

The following commands set the hello delay time to 5 seconds:

```
switch#configure terminal
```

```
switch(config)#spanning-tree hello-time 5
```

For more information about this command, see “SPANNING-TREE HELLO-TIME” on page 250.

Setting the BPDU Filter

The Spanning Tree Protocol sends BPDUs from all interfaces. Enabling the BPDU filter ensures that portfast-enabled interfaces do not transmit or receive any BPDUs. Use the SPANNING-TREE BPDU-FILTER DEFAULT command to globally enable the BPDU filter on a bridge.

The syntax of this command is:

```
spanning-tree portfast bpdu-filter default
```

The following commands enable the BPDU filter on a bridge:

```
switch#configure terminal
```

```
switch(config)#spanning-tree portfast bpdu-filter default
```

For more information about this command, see “SPANNING-TREE PORTFAST BPDU-FILTER DEFAULT” on page 253.

Setting the BPDU Guard

When the BPDU guard feature is set for a bridge, all portfast-enabled interfaces of the bridge that have the BPDU guard set to default shut down the interface on receiving a BPDU. In this case, the BPDU is not processed. You can bring the interface up manually by using the NO SHUTDOWN command. See “SHUTDOWN” on page 181.

Use the SPANNING-TREE BPDU-GUARD DEFAULT command to enable the BPDU (Bridge Protocol Data Unit) guard feature on a bridge. This command indicates the bridge level BPDU-Guard configuration takes effect.

The syntax of this command is:

```
spanning-tree portfast bpdu-guard default
```

The following commands enable the BPDU Guard feature on a bridge:

```
switch#configure terminal
```

```
switch(config)#spanning-tree portfast bpdu-guard
```

For more information about this command, see “SPANNING-TREE PORTFAST BPDU-GUARD DEFAULT” on page 254.

Configuring 802.1p Class of Service

When a port on an Ethernet switch becomes oversubscribed—its egress queues contain more packets than the port can handle in a timely manner—the port may be forced to delay the transmission of some packets, resulting in the delay of packets reaching their destinations. A port may be forced to delay transmission of packets while it handles other traffic. Some packets destined to be forwarded to an oversubscribed port from other switch ports may be discarded.

Although minor delays are often of no consequence to a network or its performance, there are applications, referred to as delay or time sensitive applications, that can be impacted by packet delays. Voice transmission and video conferencing are two examples. A delay in the transmission of packets carrying their data could impact the quality of the audio or video.

This is where CoS can be of value. What it does is it permits a switch to give higher priority to some packets over other packets.

There are two principal types of traffic found on the ports of a Gigabit Ethernet switch, one being untagged packets and the other tagged packets. As explained in “Tagged VLAN Overview” on page 257, one of the principal differences between them is that tagged packets contain VLAN information.

CoS applies mainly to tagged packets because, in addition to carrying VLAN information, these packets can also contain a priority level specifying how important (delay sensitive) a packet is in comparison to other packets. It is this number that the switch refers to when determining a packet's priority level.

The 802.1p Class of Service (CoS) feature is configured on a per port basis. The following examples show how to set this feature.

To assign a CoS ingress value to port 18 with a user-priority of 4, use the following commands:

```
switch# configure terminal
```

```
switch(config)# interface ge18
```

```
switch(config-if)# user-priority 4
```

For more information about this command, see “USER-PRIORITY” on page 193.

To assign a weight of 10 to queue 3, use the following commands:

```
switch# configure terminal
```

```
switch(config)# mls qos 0 0 0 0 0 0 10 0 0 0 0 0 0 0 0
```

Note

Repeat the MLS QOS command for each queue.

For more information about this command, see “MLS QOS” on page 143.

To set CoS mapping on port 12 with a user priority of 7 and a traffic class of 8, enter the following commands:

```
switch# configure terminal
```

```
switch(config)# interface ge12
```

```
switch(config-if)# traffic-class-table user-priority 7  
num-traffic-classes 8
```

For more information about this command, see “TRAFFIC-CLASS-TABLE USER-PRIORITY NUM-TRAFFIC-CLASSES” on page 192.

Section I

Command Modes

The chapters in this section provide information and procedures for basic switch setup using the AT-S100 Management Software. The following chapters are provided:

- ❑ Chapter 3, “Privileged Executive Mode Commands” on page 71
- ❑ Chapter 4, “Configuration Terminal Mode Commands” on page 115
- ❑ Chapter 5, “Interface Configuration Mode Commands” on page 163

Privileged Executive Mode Commands

This chapter describes the commands in the Privileged Executive mode which are used to perform general switch functions such as copying configuration file and displaying interface and MAC address table information. This chapter contains the following commands:

- ❑ “CLEAR MAC ADDRESS-TABLE DYNAMIC” on page 73
- ❑ “CLEAR MAC ADDRESS-TABLE MULTICAST” on page 75
- ❑ “CLEAR MAC ADDRESS-TABLE STATIC” on page 77
- ❑ “CONFIGURE TERMINAL” on page 79
- ❑ “COPY” on page 81
- ❑ “COPY A.B.C.D” on page 82
- ❑ “COPY DEFAULT.CFG” on page 84
- ❑ “CP” on page 86
- ❑ “DOWNLOAD TFTP” on page 87
- ❑ “EXIT” on page 88
- ❑ “LOGOUT” on page 89
- ❑ “SHOW INTERFACE” on page 90
- ❑ “SHOW MAC ADDRESS-TABLE” on page 92
- ❑ “SHOW MAC ADDRESS-TABLE AGEING-TIME” on page 94
- ❑ “SHOW MAC ADDRESS-TABLE DYNAMIC” on page 96
- ❑ “SHOW MAC ADDRESS-TABLE INTERFACE” on page 98
- ❑ “SHOW MAC ADDRESS-TABLE STATIC” on page 100
- ❑ “SHOW MAC ADDRESS-TABLE VLAN Command” on page 103
- ❑ “SHOW RUNNING-CONFIG INTERFACE” on page 104
- ❑ “SHOW SPANNING-TREE” on page 106
- ❑ “SHOW STATIC-CHANNEL-GROUP” on page 109
- ❑ “SHOW USER-PRIORITY” on page 110
- ❑ “SYSTEM FACTORY-RESET” on page 111
- ❑ “SYSTEM REBOOT” on page 112
- ❑ “UPLOAD TFTP” on page 113

Note

For VLAN-specific commands, see Chapter 11, “Virtual Local Area Networks (VLAN) Commands” on page 257.

CLEAR MAC ADDRESS-TABLE DYNAMIC

Syntax

```
clear mac address-table dynamic [address HHHH.HHHH.HHHH
|interface ge<1-28>|vlan VID
```

Parameters

address	Specifies a MAC address in the following format: HHHH.HHHH.HHHH
interface	Specifies the name of an interface. There are 28 ports on the 9000/28 and 9000/28SP switches. To specify a port, precede the port number with "ge."
VID	Specifies the VLAN ID. Use a value between 1 and 4094.

Description

Use the CLEAR MAC ADDRESS-TABLE DYNAMIC command to remove a dynamic MAC address from the switch. You can remove all of the dynamic MAC addresses, specific MAC addresses, or all MAC addresses assigned to an VLAN.

For procedures to configure and display the MAC addresses, see "Displaying and Setting MAC Addresses" on page 32.

Command Mode

Privileged Executive mode

Examples

To remove dynamic MAC address 0030.846e.bac7 from the MAC address table, use the following command:

```
switch#clear mac address-table dynamic address
0030.846e.bac7
```

To remove all dynamic MAC addresses from the MAC address table, enter the following command:

```
switch#clear mac address-table dynamic
```

Related Commands

“CLEAR MAC ADDRESS-TABLE MULTICAST” on page 75

“CLEAR MAC ADDRESS-TABLE STATIC” on page 77

CLEAR MAC ADDRESS-TABLE MULTICAST

Syntax

```
clear mac address-table multicast [address MACADDR  
| interface ge<1-28> | vlan VID]
```

Parameters

address	Specifies a multicast MAC address in the following format: HHHH.HHHH.HHHH
interface	Specifies the name of an interface. There are 28 ports on the 9000/28 and 9000/28SP switches. To specify a port, precede the port number with "ge."
VID	Specifies the VLAN ID. Use a value between 1 and 4094.

Description

Use the CLEAR MAC ADDRESS-TABLE MULTICAST command to remove a multicast MAC address from the switch. You can remove all of the multicast MAC addresses, specific multicast MAC addresses, or all multicast MAC addresses assigned to an VLAN.

For procedures to configure and display the MAC addresses, see "Displaying and Setting MAC Addresses" on page 32.

Command Mode

Privileged Executive mode

Examples

To remove multicast MAC address 0100.5100.0001 from the MAC address table, enter the following command:

```
switch#clear mac address-table multicast address  
0100.5100.0001
```

To remove all multicast MAC addresses from the MAC address table, enter the following command:

```
switch#clear mac address-table multicast
```

Related Commands

“CLEAR MAC ADDRESS-TABLE DYNAMIC” on page 73

“CLEAR MAC ADDRESS-TABLE STATIC” on page 77

CLEAR MAC ADDRESS-TABLE STATIC

Syntax

```
clear mac address-table static|address HHHH.HHHH.HHHH
|interface ge<1-28>|vlan VID
```

Parameters

address	Specifies a MAC address in the following format: HHHH.HHHH.HHHH
interface	Specifies the name of an interface. There are 28 ports on the 9000/28 and 9000/28SP switches. To specify a port, precede the port number with "ge."
VID	Specifies the VLAN ID. Use a value between 1 and 4094.

Description

Use the CLEAR MAC ADDRESS-TABLE STATIC command remove static MAC addresses from the switch. You can remove all of the static MAC addresses, specific MAC addresses, or all MAC addresses assigned to an VLAN.

For procedures to configure and display the MAC addresses, see "Displaying and Setting MAC Addresses" on page 32.

Command Mode

Privileged Executive mode

Examples

To remove static MAC address 0000.cd28.0752 from the MAC address table, enter the following command:

```
switch#clear mac address-table static address
0000.cd28.0752
```

To remove all static MAC addresses from the MAC address table, enter the following command:

```
switch#clear mac address-table static
```

Related Commands

“CLEAR MAC ADDRESS-TABLE DYNAMIC” on page 73

“CLEAR MAC ADDRESS-TABLE MULTICAST” on page 75

CONFIGURE TERMINAL

Syntax

`configure terminal`

Parameters

none

Description

Use this command to enter the Configuration Terminal command mode. After you enter this command, the command prompt changes to "(config)#" to indicate the new mode.

To exit the Configure Terminal command mode, enter EXIT or CTRL Z.

For a description of the Configuration Terminal mode, see "Configuration Terminal Mode" on page 19. For information about the commands in the Configuration Terminal mode, see Chapter 4, "Configuration Terminal Mode Commands" on page 115.

Note

It is not necessary to enter the full command. You can abbreviate this command to "config t."

Command Mode

Privileged Executive mode

Examples

To enter the Configure Terminal command mode, enter the following command:

```
switch#configure terminal
```

The prompt changes to:

```
switch(config)#
```

To use the abbreviated form of the CONFIGURE TERMINAL command mode, enter the following command:

```
switch#config t
```

The prompt changes to:

```
Switch(config)#
```

Related Commands

none

COPY

Syntax

```
copy running-config startup-config
```

Parameters

running-config Indicates the running configuration file.

startup-config Indicates the start-up configuration file.

Description

Use the COPY command to save your current configuration to the start-up configuration file, called “startup-config,” on the switch.

Command Mode

Privileged Executive mode

Examples

In the following example, the running configuration file is copied to the startup configuration file which is named “startup-config:”

```
switch#copy running-config startup-config
```

The software displays the following:

```
Building configuration...
```

```
[OK]
```

Enter the abbreviated form of the COPY command to save the current configuration on the switch to the start-up configuration file called “startup-config:”

```
switch# copy run start
```

The software displays the following:

```
Building configuration...
```

```
[OK]
```

Related Commands

“CP” on page 86

COPY A.B.C.D

Syntax

```
copy A.B.C.D SRCFILENAME DESTFILENAME
```

Parameters

A.B.C.D	Indicates an IP address in the following format: xxx.xxx.xxx.xxx
SRCFILENAME	Indicates the name of the source configuration file. This file name must end with the “.cfg” suffix.
DESTFILENAME	Indicates the name of the destination configuration file. This file name must end with the “.cfg” suffix.

Description

Use the COPY A.B.C.D command to download a configuration file from the switch onto an TFTP server. For example, you may want to download a configuration file from a backup server onto your switch. You must have the IP address of the TFTP server to set this command.

Command Mode

Privileged Executive mode

Examples

Enter the following command to download a configuration file called “jenny3.cfg” from a TFTP server with an IP address of 192.58.48.1 onto your switch. The name of the new configuration file on the switch is “at100v103.cfg:”

```
switch# copy 192.58.48.1 jenny.cfg at100v103.cfg
```

Enter the following command to download a configuration file called “test.cfg” from a TFTP server with an IP address of 192.58.48.5 onto your switch. The name of the new configuration file on the switch is “master100v103.cfg:”

```
switch# copy 192.58.48.5 test.cfg master100v103.cfg
```

Related Commands

“COPY” on page 81

“COPY DEFAULT.CFG” on page 84

“CP” on page 86

“DOWNLOAD TFTP” on page 87

“UPLOAD TFTP” on page 113

COPY DEFAULT.CFG

Syntax

```
copy default.cfg A.B.C.D FILENAME
```

Parameters

default.cfg	Indicates the name of the source configuration file. This file name must end with the “.cfg” suffix.
A.B.C.D	Indicates an IP address in the following format: xxx.xxx.xxx.xxx
FILENAME	Indicates the name of the destination configuration file. This file name must end with the “.cfg” suffix.

Description

Use the COPY DEFAULT.CFG command to upload a configuration file from the switch onto a TFTP server. You may want to upload a configuration file from your switch onto a backup server. Or, you may want to upload a configuration file from your switch to a TFTP server and then download it to other AT-9000 Series switches with the COPY A.B.C.D command. In addition, you must have the IP address of the TFTP server to set this command.

Command Mode

Privileged Executive mode

Examples

Enter the following command to upload a file called “may.cfg” from the switch onto a TFTP server with an IP address of 192.58.48.1. The new filename is “at100v103.cfg.”

```
switch# copy may.cfg 192.58.48.1 at100v103.cfg
```

Enter the following command to upload a text file called “june.cfg” from the switch onto a TFTP server with an IP address of 192.58.48.5. The new file name is “s100v103.cfg.”

```
switch# copy june.cfg 192.58.48.5 s100v103.cfg
```

Related Commands

“COPY” on page 81

“COPY A.B.C.D” on page 82

“CP” on page 86

CP

Syntax

```
cp source-file new-file
```

Parameters

source-file	Indicates the source configuration file.
new-file	Indicates the new file which becomes a copy of the source file.

Description

Use the CP command to make a copy of a configuration file and save it in the current directory on the switch.

Command Mode

Privileged Executive mode

Examples

In the following example, the running configuration file is copied to the startup configuration file which is named “frank2.cfg.”

```
switch#copy default.cfg frank2.cfg
```

You can confirm the file has been copied into the current directory with the LS command. See the following example of the output of the LS command:

```
default.cfg
```

```
frank2.cfg
```

```
ssh_host_key
```

```
ssh_host_key.pub
```

```
ssh_host_rsa_key
```

Related Commands

“COPY” on page 81

“COPY A.B.C.D” on page 82

“COPY DEFAULT.CFG” on page 84

DOWNLOAD TFTP

Syntax

```
download tftp A.B.C.D FILENAME
```

Parameters

A.B.C.D Indicates the IP address of an TFTP server. Specify the IP address in the following format:

xxx.xxx.xxx.xxx

FILENAME Specifies the filename of an image (.img) file.

Description

Use this command to download an image file from an TFTP server onto the switch. For example, you may want to use this command to download the latest version of the AT-S100 software onto your switch. You must have the IP address of the TFTP server to set this command.

Command Mode

Privileged Executive mode

Example

The following command uses a TFTP server, with an IP address of 189.11.1.1, to download the file called "ATS100_v103.img" onto the switch:

```
switch#download tftp 189.11.1.1 ATS100_v103.img
```

Related Commands

"COPY" on page 81

"COPY DEFAULT.CFG" on page 84

"UPLOAD TFTP" on page 113

EXIT

Syntax

`exit`

Parameters

none

Description

Use the EXIT command to quit the Configuration Terminal mode and enter the Privileged Executive mode. After you enter this command, the prompt changes to “Switchname#” to indicate the Privileged Executive mode.

Command Mode

Configuration Terminal mode

Example

Enter the following commands to exit the Configuration Terminal mode and return the software to the Privileged Executive mode:

```
switch#configure terminal
```

```
switch(config)#exit
```

The software displays the following prompt:

```
switch#
```

Related Commands

none

LOGOUT

Syntax

logout

Parameters

none

Description

Use the LOGOUT command to quit the Privileged Executive mode and log out of the software.

Command Mode

Privileged Executive mode

Example

The following is an example of the LOGOUT command:

```
switch#logout
```

Related Commands

none

SHOW INTERFACE

Syntax

```
show interface IFNAME ge<1-28>
```

Parameters

IFNAME Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with “ge.”

Description

Use the SHOW INTERFACE command to display the configuration and status of an interface. If you do not specify an interface, this command displays the status of all the interfaces.

Command Mode

Privileged Executive mode

Example

The following is an example of the SHOW INTERFACE command on port 1 and the sample output:

```
switch#show interface ge1

Interface ge1
  Hardware is Ethernet, address is 0004.2104.0801 (bia
004.2104.0801)
  index 2001 metric 1 mtu 1500 duplex-full arp ageing
timeout 0
  speed unknown mdix mdi
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
    input packets 013884, bytes 01642232, multicast
packets 07691 broadcast packets 06185
    64-byte packets 05968, 65-127 packets 05346, 128-255
packets 01293
    245-511 packets 01366, 512-1023 packets 03, >1024 packets
00
    dropped 00, jabber 00 CRC error 03 undersize frames 00
    oversize frames 00, fragments 00 collisions 00
  output packets 092, bytes 05898, multicast packets 092
  broadcast packets 00
```

Related Commands

“SHOW MAC ADDRESS-TABLE INTERFACE” on page 98

SHOW MAC ADDRESS-TABLE

Syntax

```
show mac address-table
```

Parameters

none

Description

Use the SHOW MAC ADDRESS-TABLE command to display the status of the static and dynamic MAC addresses assigned to the switch.

For procedures to configure and display the MAC addresses, see “Displaying and Setting MAC Addresses” on page 32.

Command Mode

Privileged Executive mode

Example

The following command displays the settings of the MAC address table:

```
switch#show mac address-table
```

See Figure 3 for an example display.

```
(switch3)# show mac address-table
Mac Address Table
```

vlan	MAC Address	Type	Ports	Forward
1	0100.5e7f.ffffa	STATIC	ge1	1
1	0000.cd14.6448	DYNAMIC	ge1	1
1	0000.f4d8.3534	DYNAMIC	ge1	1
1	0004.5a5e.6fd3	DYNAMIC	ge1	1
1	0006.5ba3.67d6	DYNAMIC	ge1	1
5	0006.5bb2.6589	DYNAMIC	ge8	1
5	0006.5bdd.6c69	DYNAMIC	ge8	1
5	0008.749c.101a	DYNAMIC	ge8	1
5	0008.74a2.04c2	DYNAMIC	ge8	1
5	0008.74cb.5fc6	DYNAMIC	ge8	1
5	0008.74d3.f02c	DYNAMIC	ge8	1
10	0008.74dd.87f7	DYNAMIC	ge12	1
10	0008.74df.29d8	DYNAMIC	ge12	1

```
(switch3)#
```

Figure 3. SHOW MAC ADDRESS-TABLE Command

The fields in Figure 3 are defined in the following list:

- ❑ **vlan.** This field indicates the VLAN ID.
- ❑ **MAC Address.** This field indicates the MAC address in the format: HHH.HHH.HHH.
- ❑ **Type.** This field indicates a static or dynamic MAC address.
- ❑ **Ports.** This field indicates the name of the port.
- ❑ **Forward.** This field indicates if data is forwarded to a MAC address or not. A value of 1 indicates data is forwarded to a MAC address. A value of 0 indicates that data is discarded and is not forwarded to a MAC address.

Related Commands

“SHOW MAC ADDRESS-TABLE AGING-TIME” on page 94

“SHOW MAC ADDRESS-TABLE DYNAMIC” on page 96

“SHOW MAC ADDRESS-TABLE INTERFACE” on page 98

“SHOW MAC ADDRESS-TABLE STATIC” on page 100

“SHOW MAC ADDRESS-TABLE VLAN” on page 102

SHOW MAC ADDRESS-TABLE AGEING-TIME

Syntax

```
show mac address-table ageing-time
```

Parameters

none

Description

Use the SHOW MAC ADDRESS-TABLE AGEING-TIME command to display the aging time of MAC addresses assigned to the switch. By default, this value is set to 300 seconds (5 minutes).

The switch uses the aging timer to delete inactive dynamic MAC addresses from the MAC address table. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. Deleting aged-out MAC addresses prevents the table from becoming full of addresses of inactive nodes.

When the aging timer is set to 0, it disables the timer. No dynamic MAC addresses are aged out and the table stops learning new addresses after reaching its maximum capacity.

For procedures to configure and display the MAC addresses, see “Displaying and Setting MAC Addresses” on page 32.

Command Mode

Privileged Executive mode

Example

The following command displays the MAC address aging-time:

```
switch#show mac address-table ageing-time
```

See Figure 4 for an example display.

```
(switch3)# show mac address-table aging-time
Aging-time 300

(switch3)#
```

Figure 4. SHOW MAC ADDRESS-TABLE AGING-TIME

Related Commands

“SHOW MAC ADDRESS-TABLE” on page 92

“SHOW MAC ADDRESS-TABLE DYNAMIC” on page 96

“SHOW MAC ADDRESS-TABLE INTERFACE” on page 98

“SHOW MAC ADDRESS-TABLE STATIC” on page 100

“SHOW MAC ADDRESS-TABLE VLAN” on page 102

SHOW MAC ADDRESS-TABLE DYNAMIC

Syntax

```
show mac address-table dynamic |
begin|exclude|include|redirect
```

Parameters

dynamic	Indicates the dynamic MAC addresses.
	Specifies output variables. Choose from the following options:
begin	Indicates to begin with a line that matches.
exclude	Specifies to exclude lines that match.
include	Specifies to include lines that match.
redirect	Indicates to redirect the output.

Description

Use the SHOW MAC ADDRESS-TABLE DYNAMIC command to display the status of the static and dynamic MAC addresses assigned to the switch.

For procedures to configure and display the MAC addresses, see “Displaying and Setting MAC Addresses” on page 32.

Command Mode

Privileged Executive mode

Example

The following command displays the dynamic MAC addresses:

```
switch#show mac address-table dynamic
```


See Figure 6 for a sample display.

```
(switch3)# show mac address-table dynamic
Mac Address Table
```

Vlan	MAC Address	Type	Ports	Forward
1	0000.cd14.6448	DYNAMIC	ge3	1
1	0000.f4d8.3534	DYNAMIC	ge3	1
1	0004.5a5e.6fd3	DYNAMIC	ge3	1
1	0006.5ba3.67d6	DYNAMIC	ge3	1
1	0006.5bb2.6589	DYNAMIC	ge3	1
1	0006.5bdd.6c69	DYNAMIC	ge3	1
1	0008.749c.101a	DYNAMIC	ge3	1
1	0008.74a2.04c2	DYNAMIC	ge3	1
1	0008.74cb.5fc6	DYNAMIC	ge3	1
1	0008.74d3.f02c	DYNAMIC	ge3	1
1	0008.74dd.87f7	DYNAMIC	ge3	1

```
(switch3)#
```

Figure 5. SHOW MAC ADDRESS-TABLE DYNAMIC Command

The fields in Figure 6 are defined in the following list:

- ❑ **vlan.** This field indicates the VLAN ID.
- ❑ **MAC Address.** This field indicates the MAC address in the format: HHH.HHH.HHH.
- ❑ **Type.** This field indicates a static or dynamic MAC address.
- ❑ **Ports.** This field indicates the name of the port.
- ❑ **Forward.** This field indicates if data is forwarded to a MAC address or not. A value of 1 indicates data is forwarded to a MAC address. A value of 0 indicates that data is discarded and is not forwarded to a MAC address.

Related Commands

“SHOW MAC ADDRESS-TABLE” on page 92

“SHOW MAC ADDRESS-TABLE AGEING-TIME” on page 94

“SHOW MAC ADDRESS-TABLE INTERFACE” on page 98

“SHOW MAC ADDRESS-TABLE STATIC” on page 100

“SHOW MAC ADDRESS-TABLE VLAN” on page 102

SHOW MAC ADDRESS-TABLE INTERFACE

Syntax

```
show mac address-table interface ge<1-28>
```

Parameters

interface	Specifies the name of an interface. There are 28 ports on the 9000/28 and 9000/28SP switches. To specify a port, precede the port number with “ge.”
-----------	---

Description

Use the SHOW MAC ADDRESS-TABLE INTERFACE command to display the status of the static and dynamic MAC addresses assigned to a port.

For procedures to configure and display the MAC addresses, see “Displaying and Setting MAC Addresses” on page 32.

Command Mode

Privileged Executive mode

Example

The following command displays the settings of the MAC address table on port 3:

```
switch#show mac address-table interface ge3
```

See Figure 6 for an example display.

```
(switch3)# show mac address-table interface ge3
Mac Address Table
```

Vlan	MAC Address	Type	Ports	Forward
1	0100.5e7f.ffffa	STATIC	ge3	1
1	0000.cd14.6448	DYNAMIC	ge3	1
1	0000.f4d8.3534	DYNAMIC	ge3	1
1	0004.5a5e.6fd3	DYNAMIC	ge3	1
1	0006.5ba3.67d6	DYNAMIC	ge3	1
1	0006.5bb2.6589	DYNAMIC	ge3	1
1	0006.5bdd.6c69	DYNAMIC	ge3	1
1	0008.749c.101a	DYNAMIC	ge3	1
1	0008.74a2.04c2	DYNAMIC	ge3	1
1	0008.74cb.5fc6	DYNAMIC	ge3	1
1	0008.74d3.f02c	DYNAMIC	ge3	1
1	0008.74dd.87f7	DYNAMIC	ge3	1

```
(switch3)#
```

Figure 6. SHOW MAC ADDRESS-TABLE INTERFACE Command

The fields in Figure 6 are defined in the following list:

- ❑ **vlan.** This field indicates the VLAN ID.
- ❑ **MAC Address.** This field indicates the MAC address in the format: HHH.HHH.HHH.
- ❑ **Type.** This field indicates a static or dynamic MAC address.
- ❑ **Ports.** This field indicates the name of the port.
- ❑ **Forward.** This field indicates if data is forwarded to a MAC address or not. A value of 1 indicates data is forwarded to a MAC address. A value of 0 indicates that data is discarded and is not forwarded to a MAC address.

Related Commands

“SHOW MAC ADDRESS-TABLE” on page 92

“SHOW MAC ADDRESS-TABLE AGEING-TIME” on page 94

“SHOW MAC ADDRESS-TABLE DYNAMIC” on page 96

“SHOW MAC ADDRESS-TABLE STATIC” on page 100

“SHOW MAC ADDRESS-TABLE VLAN” on page 102

SHOW MAC ADDRESS-TABLE STATIC

Syntax

```
show mac address-table static |  
(begin|exclude|include|redirect) > WORD
```

Parameters

<code>static</code>	Indicates the static MAC addresses.
<code> </code>	Specifies output variables. Choose from the following options:
<code>begin</code>	Indicates to begin with a line that matches.
<code>exclude</code>	Specifies to exclude lines that match.
<code>include</code>	Specifies to include lines that match.
<code>redirect</code>	Indicates to redirect the output.
<code>></code>	Redirects the output of the command to a file name.

Description

Use the SHOW MAC ADDRESS-TABLE STATIC command to display the status of the static MAC addresses assigned to the switch.

For procedures to configure and display the MAC addresses, see “Displaying and Setting MAC Addresses” on page 32.

Command Mode

Privileged Executive mode

Example

The following command displays the settings of the static MAC addresses:

```
switch#show mac address-table static
```

See Figure 7 for an example display.

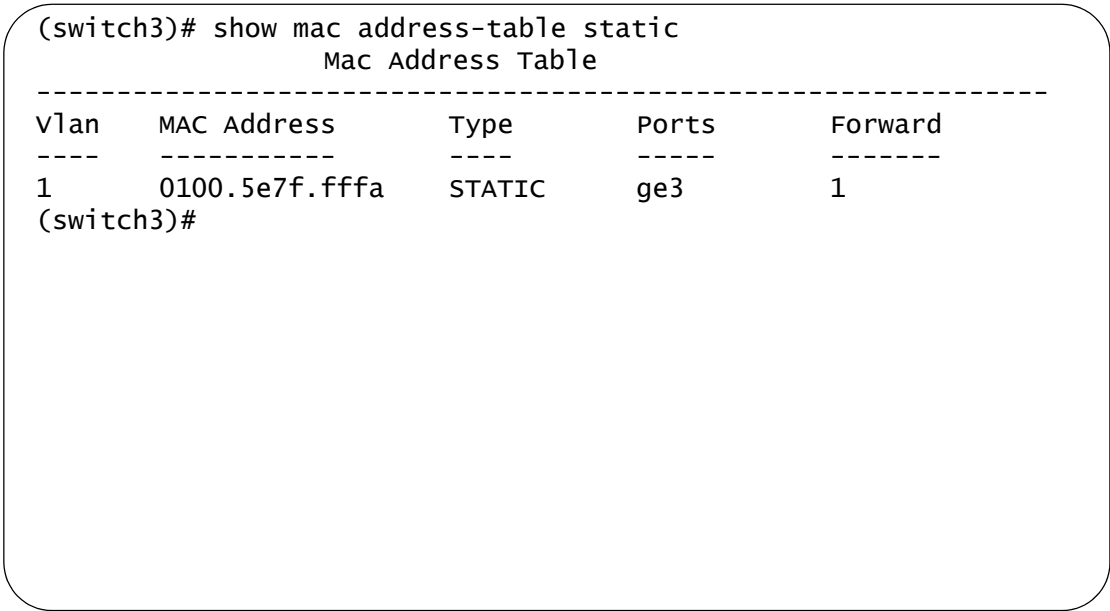


Figure 7. SHOW MAC ADDRESS-TABLE STATIC

The fields in Figure 8 are defined in the following list:

- ❑ **vlan.** This field indicates the VLAN ID.
- ❑ **MAC Address.** This field indicates the MAC address in the format: HHH.HHH.HHH.
- ❑ **Type.** This field indicates a static or dynamic MAC address.
- ❑ **Ports.** This field indicates the name of the port.
- ❑ **Forward.** This field indicates if data is forwarded to a MAC address or not. A value of 1 indicates data is forwarded to a MAC address. A value of 0 indicates that data is discarded and is not forwarded to a MAC address.

Related Commands

- “SHOW MAC ADDRESS-TABLE” on page 92
- “SHOW MAC ADDRESS-TABLE AGEING-TIME” on page 94
- “SHOW MAC ADDRESS-TABLE DYNAMIC” on page 96
- “SHOW MAC ADDRESS-TABLE INTERFACE” on page 98
- “SHOW MAC ADDRESS-TABLE VLAN” on page 102

SHOW MAC ADDRESS-TABLE VLAN

Syntax

```
show mac address-table vlan <1-4094>
```

Parameters

vlan Specifies a VLAN ID. Enter a value between 1 and 4094.

Description

Use the SHOW MAC ADDRESS-TABLE VLAN command to display the status of both the static and dynamic MAC addresses assigned to the switch.

For procedures to configure and display the MAC addresses, see “Displaying and Setting MAC Addresses” on page 32.

Command Mode

Privileged Executive mode

Example

The following command displays the MAC address configuration on VLAN 1:

```
switch#show mac address-table vlan 1
```

See Figure 8 on page 103 for a sample display.

```
(switch3)# show mac address-table vlan 1
Mac Address Table
```

vlan	MAC Address	Type	Ports	Forward
1	0100.5e7f.ffffa	STATIC	ge1	1
1	0000.cd14.6448	DYNAMIC	ge1	1
1	0000.f4d8.3534	DYNAMIC	ge1	1
1	0004.5a5e.6fd3	DYNAMIC	ge1	1
1	0006.5ba3.67d6	DYNAMIC	ge1	1
1	0006.5bb2.6589	DYNAMIC	ge8	1
1	0006.5bdd.6c69	DYNAMIC	ge8	1
1	0008.749c.101a	DYNAMIC	ge8	1
1	0008.74a2.04c2	DYNAMIC	ge8	1
1	0008.74cb.5fc6	DYNAMIC	ge8	1
1	0008.74d3.f02c	DYNAMIC	ge8	1
1	0008.74dd.87f7	DYNAMIC	ge12	1
1	0008.74df.29d8	DYNAMIC	ge12	1
1	0008.74f0.9377	DYNAMIC	ge12	1
1	0008.74fe.f3f3	DYNAMIC	ge12	1

Figure 8. SHOW MAC ADDRESS-TABLE VLAN Command

The fields in Figure 8 are defined in the following list:

- ❑ vlan. This field indicates the VLAN ID.
- ❑ MAC Address. This field indicates the MAC address in the format: HHH.HHH.HHH.
- ❑ Type. This field indicates a static or dynamic MAC address.
- ❑ Ports. This field indicates the name of the port.
- ❑ Forward. This field indicates if data is forwarded to a MAC address or not. A value of 1 indicates data is forwarded to a MAC address. A value of 0 indicates that data is discarded and is not forwarded to a MAC address.

Related Commands

“SHOW MAC ADDRESS-TABLE” on page 92

“SHOW MAC ADDRESS-TABLE AGEING-TIME” on page 94

“SHOW MAC ADDRESS-TABLE DYNAMIC” on page 96

“SHOW MAC ADDRESS-TABLE INTERFACE” on page 98

“SHOW MAC ADDRESS-TABLE STATIC” on page 100

SHOW RUNNING-CONFIG INTERFACE

Syntax

```
show running-config interface INTERFACE
```

Parameters

IFNAME Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with “ge.” To specify a VLAN, use the VLAN ID.

Note

Do not mix interface types in a list. Also, the specified interfaces must exist.

Description

Use the SHOW RUNNING-CONFIG INTERFACE command to display the current configuration of one or more interfaces on the device.

Command Mode

All modes

Examples

To display the status of the SHOW RUNNING-CONFIG INTERFACE command on port 4:

```
switch#show running-config interface ge4
```

See Figure 13 for an example display.

```
(switch3)# show running-config interface ge4
!
interface ge4
    static channel-group 3
```

Figure 9. SHOW RUNNING-CONFIG INTERFACE Port Example

To display the status of the current running configuration of a switch for VLAN 2:

```
switch#show running-config interface vlan2
```

See Figure 13 for an example display.

```
(switch3)# show running-config interface vlan2
!  
interface vlan2  
!
```

Figure 10. SHOW RUNNING-CONFIG INTERFACE VLAN Example

Related Commands

“SHOW RUNNING-CONFIG” on page 153

SHOW SPANNING-TREE

Syntax

```
show spanning-tree interface INTERFACE
```

Parameters

IFNAME Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with “ge.”

Description

Use the SHOW SPANNING-TREE command to display the status of the active spanning tree protocol on the specified port.

For procedures to configure the spanning tree protocols, see “Setting STP and RSTP” on page 62.

Command Mode

Privileged Executive mode

Example

The following command displays the spanning tree configuration on port 1:

```
switch#show spanning-tree interface ge1
```

This command displays a variety of parameters. An example of page 1 of the display is shown in Figure 11 on page 107.

```
(switch3)# show spanning-tree interface ge1
% 1: Bridge up - Spanning Tree Disabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000012341212ab
% 1: Bridge Id 80000012341212ab
% 1: last topology change Sat Jan 1 00:00:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% 1:   ge1: Port 2001 - Id 87d1 - Role Disabled - State Fwd
% 1:   ge1: Designated Path Cost 0
% 1:   ge1: Configured Path Cost 200000 - Add type Explicit ref
count 1
% 1:   ge1: Designated Port Id 87d1 - Priority 128 -
% 1:   ge1: Root 80000012341212ab
% 1:   ge1: Designated Bridge 80000012341212ab
% 1:   ge1: Message Age 0 - Max Age 20
% 1:   ge1: Hello Time 2 - Forward Delay 15
% 1:   ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 -
topo change timer 0
% 1:   ge1: forward-transitions 2
% 1:   ge1: Version Rapid Spanning Tree Protocol - Received None
Send RSTP
--More--
```

Figure 11. SHOW SPANNING-TREE Command, page 1

See Figure 12 for page 2 of the display.

```
% 1:   ge1: No portfast configured - Current portfast off
% 1:   ge1: portfast bpdu-guard default - Current portfast bpdu-
guard off
% 1:   ge1: portfast bpdu-filter default - Current portfast bpdu-
guard off
% 1:   ge1: no root guard configured - Current root guard off
% 1:   ge1: Configured Link Type point-to-point - Current point-
to-point
%
(switch3)#
```

Figure 12. SHOW SPANNING-TREE Command, page 2

Related Commands

See Chapter 10, “Spanning Tree Protocol (STP) Commands” on page 243.

SHOW STATIC-CHANNEL-GROUP

Syntax

```
show static-channel-group
```

Parameters

none

Description

Use the SHOW STATIC-CHANNEL-GROUP command to display the static-channel groups configured on the switch.

For a procedure to set create static port trunks, see “Creating Static Trunks” on page 49.

Command Mode

Privileged Executive mode

Example

The following example shows the SHOW STATIC-CHANNEL-GROUP command and a sample of the output:

```
switch3#show static-channel-group
```

See Figure 13 for an example display.

```
(switch3)# show static-channel-group
Static Aggregator: sa3
Type: src-dst-mac
Member: ge9
(switch3)#
```

Figure 13. SHOW STATIC-CHANNEL-GROUP

Related Commands

“STATIC-CHANNEL-GROUP” on page 184

SHOW USER-PRIORITY

Syntax

```
show user-priority interface INTERFACE
```

Parameters

IFNAME Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with “ge.”

Description

Use the SHOW USER-PRIORITY command to display the user priority value on the specified port.

Command Mode

Privileged Executive mode

Example

The following command displays the user-priority value on port 8:

```
switch#show user-priority interface ge8
```

The following is an example display:

```
Default user priority: 7
```

Related Commands

“USER-PRIORITY” on page 193

SYSTEM FACTORY-RESET

Syntax

system factory-reset

Parameters

none

Description

Use the SYSTEM FACTORY-RESET command to reset the AT-S100 software to the factory default settings. When you enter this command, you will lose the running configuration.



Caution

Before you enter this command, you may want to copy your current configuration. See “COPY” on page 81.

Command Mode

Privileged Executive mode

Example

The following command sets the AT-S100 software to the factory default settings:

```
switch# system factory-reset
```

You are prompted with the following questions:

```
will lose running configuration and system will reboot?  
(Y/N)
```

To continue, enter Y for yes.

Related Commands

“COPY” on page 81

“SYSTEM REBOOT” on page 112

SYSTEM REBOOT

Syntax

`system reboot`

Parameters

none

Description

Use the SYSTEM REBOOT command to reboot the switch.

Command Mode

Privileged Executive mode

Example

The following command reboots the switch:

```
switch# system reboot
```

Related Commands

“SYSTEM FACTORY-RESET” on page 111

UPLOAD TFTP

Syntax

```
upload tftp A.B.C.D WORD
```

Parameters

A.B.C.D	Indicates an IP address in the following format: xxx.xxx.xxx.xxx
WORD	Indicates the file name of the image (.img) file on the TFTP server after you have set the UPLOAD command.

Description

Use the UPLOAD TFTP command to upload the image file from the switch onto an TFTP server. For example, you may want to use this command to create a backup copy of the AT-S100 software. You must have the IP address of the TFTP server to set this command.

You do not need to know the name of the image file on the switch to upload it. The filename that you specify in the UPLOAD command indicates the filename on the TFTP server. As a result, you can name it anything you'd like as long as the suffix is ".img."

Note

Create a dummy file on the TFTP server with the same file name as the file on the switch that you want to upload before you enter the UPLOAD command. If you do not first create the dummy file, you will receive an error message. However, the file will upload successfully.

Command Mode

Privileged Executive mode

Example

Enter the following command to upload the image file from the switch onto a TFTP server with an IP address of 192.58.48.10 and filename of "at100v103.img:"

```
switch# upload tftp 192.58.48.10 at100v103.img
```

The switch displays the following which indicates a successful upload operation:

```
TFTP IP 192.58.48.10, file name at100v103.img
```

Related Commands

“COPY” on page 81

“COPY DEFAULT.CFG” on page 84

“DOWNLOAD TFTP” on page 87

Chapter 4

Configuration Terminal Mode Commands

The commands in this chapter are accessed through the Configuration Terminal mode. The commands in this mode allow you to configure debugging, MAC addresses, and Network Time Protocol (NTP) commands.

This chapter contains the following commands:

- ❑ “CLOCK SUMMER-TIME RECURRING” on page 117
- ❑ “CLOCK TIMEZONE” on page 119
- ❑ “CRYPTO KEY GENERATE USERKEY” on page 121
- ❑ “DOT1X SYSTEM-AUTH-CTRL” on page 123
- ❑ “ENABLE PASSWORD” on page 124
- ❑ “ENABLE SECRET” on page 125
- ❑ “EXIT” on page 126
- ❑ “HOSTNAME” on page 128
- ❑ “INTERFACE” on page 129
- ❑ “IP IGMP SNOOPING” on page 131
- ❑ “IP ROUTE” on page 132
- ❑ “IP SSH RSA KEYPAIR-NAME” on page 133
- ❑ “IP SSH VERSION” on page 134
- ❑ “LINE CONSOLE” on page 135
- ❑ “LINE VTY” on page 136
- ❑ “MAC ADDRESS-TABLE AGEING-TIME” on page 138
- ❑ “MAC ADDRESS-TABLE STATIC DISCARD” on page 139
- ❑ “MAC ADDRESS-TABLE STATIC FORWARD” on page 141
- ❑ “MLS QOS” on page 143
- ❑ “NTP AUTHENTICATE” on page 145
- ❑ “NTP AUTHENTICATION-KEY” on page 146
- ❑ “NTP SERVER” on page 148
- ❑ “NTP TRUSTED-KEY” on page 150
- ❑ “SHOW LIST” on page 151
- ❑ “SHOW RUNNING-CONFIG” on page 153

- ❑ “SHOW RUNNING-CONFIG COMMUNITY-LIST” on page 158
- ❑ “SHOW RUNNING-CONFIG INTERFACE” on page 160
- ❑ “USERNAME” on page 162

Note

For GVRP-specific commands, see Chapter 7, “GVRP Commands” on page 211

Note

For VLAN-specific commands, see Chapter 11, “Virtual Local Area Networks (VLAN) Commands” on page 257.

CLOCK SUMMER-TIME RECURRING

Syntax

```
clock summer-time ZONENAME recurring START-WEEK START-
DAY START-MONTH START-TIME END-WEEK END-DAY END-MONTH
END-TIME <1-180>
```

```
no clock summer-time
```

Parameters

ZONENAME	Describes the summertime zone, up to 6 characters long.
recurring	Specifies that this summertime setting applies every year from now on.
START-WEEK	Indicates the week of the month when summertime starts in the range of 1 to 5. The value of 5 indicates the last week that has specified day in it for the specified month. For example, to start summertime on the last Sunday of the month, enter 5 for START-WEEK and "sun" for START-DAY.
START-DAY	Indicates the day of the week when summertime starts. Use the first three letters of each day of the week. Valid values are "mon," "tue," "wed," "thu," "fri," "sat," and "sun."
START-MONTH	Specifies the month that summer time starts. Use the first three letters of each month to indicate the name of a month. Valid values are "jan," "feb," "mar," "apr," "may," "jun," "jul," "aug," "sep," "oct," "nov," and "dec."
START-TIME	Indicates the time of day that summer time starts in 24-hour format: HH:MM where H represents hours and M represents minutes.
END-WEEK	Indicates the week of the month when summer time ends in the range of 1 through 5. The value of 5 indicates the last week of the month.
END-DAY	Specifies the day of the week when summer time ends. Use the first three letters of each day of the week. Valid values are "mon," "tue," "wed," "thu," "fri," "sat," and "sun."

END-MONTH	Specifies the month that summer time ends. Use the first three letters of each month to indicate the name of a month. Valid values are "jan," "feb," "mar," "apr," "may," "jun," "jul," "aug," "sep," "oct," "nov," and "dec."
END-TIME	Indicates the time of day that summer time end in 24-hour format: HH:MM where H represents hours and M represents minutes.
<1-180>	Indicates the time offset in minutes.

Description

Use the `CLOCK SUMMER-TIME RECURRING` command to define the start and end of daylight savings time for every year. In addition, this command allows you to specify the offset value to Standard Time.

The **no** parameter added to this command removes the summertime setting from the software, including the recurring dates.

Command Mode

Configuration Terminal mode

Example

To set a summer time definition for New Zealand using the official NZST (UTC+12:00) as the standard time and NZST (UTC+13:00) as summertime, with summertime set to start on the first Sunday in October and end on the third Sunday in March, use the following commands:

```
switch#configure terminal
switch(config)#clock summer-time NZDT recurring 1 sun
oct 2:00 3 sun mar 2:00 60
```

Related Commands

"`CLOCK TIMEZONE`" on page 119

"`NTP AUTHENTICATE`" on page 145

CLOCK TIMEZONE

Syntax

```
clock timezone <timezone> minus|plus <0-12>
no clock timezone
```

Parameters

timezone	Specifies a description of the timezone up to 6 characters in length.
minus	Indicates the timezone is behind UTC.
plus	Indicates the timezone is ahead of UTC.
<0-12>	Specifies the offset, in hours, from UTC.

Description

Use the CLOCK TIMEZONE command to define the clock timezone in hours. The timezone is set as an offset to the UTC of up to 12 hours. By default, the system time is set to UTC.



Caution

Configure the time zone **before** setting the local time on the system. If you set the time zone after setting the local time, the software applies the new offset to the local time.

Use the no parameter to reset the system time to UTC.

Command Mode

Configuration Terminal mode

Examples

To set the time zone to New Zealand Standard Time with an offset from UTC of +12 hours, use the following commands:

```
switch#configure terminal
switch(config)#clock timezone NZST plus 12
```

To return the time zone to UTC with no offsets, use the following commands:

```
switch#configure terminal
```

```
switch(config)#no clock timezone
```

Related Commands

“CLOCK SUMMER-TIME RECURRING” on page 117

CRYPTO KEY GENERATE USERKEY

Syntax

```
crypto key generate userkey USERNAME rsa <768-32768>
no crypto key generate userkey
```

Parameters

USERNAME	Specifies the name of the user. This parameter must begin with a letter. Valid characters are all numbers, letters, and underscores, hyphens, and periods.
rsa	Creates an RSA userkey for SSH version 2 connections.
<768-32768>	The length, in bits, of the generated key. The default is 1,024 bits.

Description

Use the CRYPTO KEY GENERATE USERKEY command to generate public and private keys for an SSH user using the RSA cryptography algorithm. To use public key authentication, copy the public key of the user onto the remote SSH server.



Caution

This command is not saved in the software configuration. However, the device saves the keys generated by this command in the non-volatile memory.

Command Mode

Configuration Terminal mode

Examples

To generate a 2048-bit RSA user key for SSH version 2 connections for a user named "bob," use the following commands:

```
switch#configure terminal
switch(config)#crypto key generate userkey bob rsa
2048
```

To generate an RSA user key for a user named “lapo,” use the following commands:

```
switch#configure terminal
```

```
switch(config)#crypto key generate userkey lapo rsa
```

Related Commands

none

DOT1X SYSTEM-AUTH-CTRL

Syntax

```
dot1x system-auth-ctrl
```

Parameters

system-auth-ctrl Enable global interface authentication.

Description

Use the DOT1X SYSTEM-AUTH-CTRL command to enable authentication globally on interfaces 1 through 28. Global authentication is disabled by default.

Command Mode

Configuration Terminal mode

Example

The following commands enable 802.1x Port Based Access Control on all interfaces:

```
switch#configure terminal
```

```
switch(config)#dot1x system-auth-ctrl
```

Related Commands

“SHOW DOT1X ALL” on page 204

ENABLE PASSWORD

Syntax

```
enable password (8) LINE
```

Parameters

- | | |
|------|--|
| 8 | Specifies a hidden password will follow. This is an optional parameter. |
| LINE | Specifies a password for the Privileged Executive Mode. Enter an alphanumeric value. |

Description

Use the ENABLE PASSWORD command to assign a password for the commands in the Privileged Executive mode. By default, there is no password assigned for this mode. For information about the Privileged Executive mode commands, see “Privileged Executive Command Mode” on page 18.

Command Mode

Configuration Terminal mode

Example

The following commands assign the Privileged Executive mode password to “rose7:”

```
switch#configure terminal
```

```
switch(config)#enable password rose7
```

Related Commands

“ENABLE SECRET” on page 125

ENABLE SECRET

Syntax

`enable secret (8) LINE`

Parameters

- | | |
|------|--|
| 8 | Specifies a hidden password will follow. This is an optional parameter. |
| LINE | Specifies a password for the Privileged Executive Mode. Enter an alphanumeric value. |

Description

Use the ENABLE SECRET command to assign a privileged-level password, or secret. By default, there is no secret assigned. For information about the Privileged Executive mode commands, see “Privileged Executive Command Mode” on page 18.

Command Mode

Configuration Terminal mode

Example

The following command assigns “aloha5551212” as the hidden password:

```
switch#configure terminal
switch(config)#enable secret 8 aloha5551212
```

Related Commands

“ENABLE PASSWORD” on page 124

EXIT

Syntax

`exit`

Parameters

none

Description

Use the EXIT command to quit the Configuration Terminal mode and enter the Privileged Executive mode. After you enter this command, the prompt changes to “Switchname#” to indicate the Privileged Executive mode.

Command Mode

Configuration Terminal mode

Example

The following commands exit the Configuration Terminal mode and returns the software to the Privileged Executive mode:

```
switch#configure terminal
```

```
switch(config)#exit
```

```
switch#
```

Related Commands

none

HELP

Syntax

help

Parameters

none

Description

Use this command to display information about the CLI. The HELP command provides information about the current parameter. There are two forms of the HELP command:

- ❑ Full help is available when you enter a command followed by a space and the question mark (?). This displays all of the parameters for the command.
- ❑ Partial help is available when you enter an abbreviated command or argument immediately followed by the question mark (?) without a space. For example, "show con?" In this case, the software responds by displaying, "SHOW CONFIGURE."

Command Mode

All modes

Examples

The following is an example of full help and the resulting display:

```
switch#clear ?
ip                Internet Protocol (IP)
mac               Clear layer 2 MAC entries
spanning-tree    spanning-tree
```

The following is an example of the partial help and the resulting display:

```
switch#snmp-server u?
switch#snmp-server user
```

Related Commands

none

HOSTNAME

Syntax

hostname NAME

Parameters

NAME Specifies the name of the switch. Enter a value between 1 and 63 alphanumeric characters. Names must start with a letter and end with a letter or digit. Within the interior of the name, there must only be letters, digits, and hyphens.

Description

Use the HOSTNAME command to assign a name to the switch. Enter a value between 1 and 63 alphanumeric characters. The name must follow the rules for ARPNET host names.

After you name the switch, the prompt changes to include the name. The new name of the switch appears in all of the command modes.

Command Mode

Configuration Terminal mode

Example

The following example assigns “Switch3” as the name of the switch and displays the new prompt:

```
none#configure terminal
none(config)#hostname Switch3
switch3(config)#
```

Related Commands

none

INTERFACE

Syntax

```
interface IFNAME
```

Parameters

IFNAME Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with "ge."

Description

Use the INTERFACE command to access the Interface Configuration command mode for the interface specified. After you enter the INTERFACE command, "-if" is added to the prompt. For more information about the commands included in the Interface mode, see "Interface Configuration Command Mode" on page 20.

Command Mode

Configuration Terminal mode

Examples

The following commands access the Interface mode on interface 3 and the resulting display:

```
switch#configure terminal
switch(config)#interface ge3
switch(config-if)#
```

The following commands access the Interface mode on interface 8 and the resulting display:

```
switch#configure terminal
switch(config)#interface ge8
switch(config-if)#
```

The following commands access the Interface mode on VLAN 1 and the resulting display (By default, all of the ports are assigned to VLAN 1.):

```
switch#configure terminal
```

```
switch(config)#interface vlan1
```

```
switch(config-if)#
```

Related Commands

“SHOW MAC ADDRESS-TABLE INTERFACE” on page 98

IP IGMP SNOOPING

Syntax

```
ip igmp snooping  
no ip igmp snooping
```

Description

Use the IP IGMP SNOOPING command to enable IGMP Snooping on the switch. When you enter this command at the Configuration Terminal mode, IGMP Snooping is enabled on the switch. By default, the IP IGMP Snooping feature is enabled.

Use the no parameter with this command to globally disable IGMP Snooping for the specified interface.

Command Mode

Configuration Terminal mode

Example

Use the following commands to enable IGMP Snooping on the switch:

```
switch#configure terminal  
switch(config)#ip igmp snooping
```

Related Commands

none

IP ROUTE

Syntax

```
ip route (GATEWAYIP|INTERFACE)
```

```
no ip route (GATEWAYIP|INTERFACE)
```

Parameters

GATEWAYIP	Indicates the IPV4 address and subnet mask of the gateway device in the following format: 000.000.000/0
INTERFACE	Specifies a the name of the interface (in the range of ge1 through ge28) that connects your device to the network.

Description

Use the IP ROUTE command to add a gateway address to the switch. Use the no form of this command to remove the static route from the switch.

Command Mode

Configuration Terminal mode

Examples

The following example sets the gateway IP address to 0.0.0.0 and a subnet mask of 0:

```
switch#configure terminal
```

```
switch(config)#ip route 0.0.0.0/0
```

Related Commands

“IP ADDRESS” on page 117

“IP ADDRESS DHCP” on page 119

IP SSH RSA KEYPAIR-NAME

Syntax

```
ip ssh rsa keypair-name WORD  
no ip ssh rsa keypair-name
```

Parameters

WORD Specifies a name of an RSA keypair.

Description

Use the IP SSH RSA KEYPAIR-NAME command to set the name of an RSA keypair.

Use the no form of this command to remove an RSA keypair.

Command Mode

Configuration Terminal mode

Example

The following commands set the keypair name to "ssh_host_rsa_key5:"

```
switch#configure terminal  
switch(config)#ip ssh rsa keypair-name  
ssh_host_rsa_key5
```

Related Commands

"IP SSH VERSION" on page 134

IP SSH VERSION

Syntax

```
ip ssh version 1|2
```

```
no ip ssh version 1|2
```

Parameters

version Indicates the SSH version number. Choose from the following options:

- 1 Specifies SSH version 1.
- 2 Specifies SSH version 2.

Description

Use the IP SSH VERSION command to set the SSH protocol version number.

Use the no form of this command to set the SSH version number to its default value.

Command Mode

Configuration Terminal mode

Example

The following commands set the switch to SSH version 2:

```
switch#configure terminal
```

```
switch(config)#ip ssh version 2
```

Related Commands

“IP SSH RSA KEYPAIR-NAME” on page 133

LINE CONSOLE

Syntax

```
line console 0
```

Parameters

none

Description

The LINE CONSOLE command sets the console configuration and enters the Line mode. The primary terminal line is set to line number 0. After you enter this command, the prompt changes to “switch(config-line)#” to indicate the Line mode.

For more information about the LINE mode, see “Line Mode Commands” on page 22.

Command Mode

Configuration Terminal mode

Example

The following commands set the primary line console to 0:

```
switch#configure terminal
switch(config)#line console 0
switch(config-line)#
```

Related Commands

“LOGIN REMOTELOCAL” on page 200

“LINE VTY” on page 136

LINE VTY

Syntax

```
line vty FIRST <0-871> LAST <0-871>
```

```
no line vty FIRST <0-871> LAST <0-871>
```

Parameters

FIRST Specifies the first line number. Enter a value between 0 and 871.

LAST Specifies the last line number. Enter a value between 0 and 871.

Description

Use the LINE VTY command to Telnet from the serial port to the RTM or to any protocol daemon. This command is necessary for all Telnet sessions. Before starting the daemon, add the value of the LINE VTY command to the daemon's configuration file. By default, there are 4 active sessions for Telnet and the web interfaces.

After you enter the LINE VTY command, the prompt changes to indicate the software has entered the Line mode. For more information about this mode, see "Line Mode Commands" on page 20.

To disable active sessions, use the no form of this command.

To display the current number of sessions, use the SHOW RUNNING-CONFIG command.

Command Mode

Configuration Terminal mode

Examples

The following commands shows the use of the LINE VTY command to enter the Line mode:

```
switch#configure terminal
```

```
switch(config)#line vty 0 15
```

```
switch(config-line)#
```


To disable Telnet and web server sessions, enter the following commands:

```
switch#configure terminal
```

```
switch(config)#line vty 0 4
```

Related Commands

“LINE CONSOLE” on page 135

“SHOW RUNNING-CONFIG” on page 153

MAC ADDRESS-TABLE AGEING-TIME

Syntax

```
mac address-table ageing-time <10-1000000>
```

```
no mac address-table ageing-time
```

Parameters

ageing-time	Indicates the ageing time in seconds. Choose a value between 10 and 1,000,000 seconds. The default is 300 seconds.
-------------	--

Description

Use the MAC ADDRESS-TABLE AGEING-TIME command to specify the ageing time for an entry in a MAC address table. Use the no form to reset this parameter.

For procedures to configure and display the MAC addresses, see “Displaying and Setting MAC Addresses” on page 32.

Command Mode

Configuration Terminal mode

Examples

The following example sets the ageing time to 120 seconds:

```
switch# configure terminal
```

```
switch#(config)# mac address-table ageing-time 120
```

Related Commands

“MAC ADDRESS-TABLE AGEING-TIME” on page 138

“MAC ADDRESS-TABLE STATIC DISCARD” on page 139

“MAC ADDRESS-TABLE STATIC FORWARD” on page 141

MAC ADDRESS-TABLE STATIC DISCARD

Syntax

```
mac address-table static MAC discard interface IFNAME
vlan VLANID
```

```
no mac address-table static
```

Parameters

MAC	Indicates the static MAC address in the following format: MMMM.MMMM.MMMM
IFNAME	Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with "ge."
VLANID	Indicates the VLAN interface. Enter a value between 2 and 4,094. If you do not enter a value, VLAN 1 is assumed by default.

Description

Use the MAC ADDRESS-TABLE STATIC DISCARD command to delete an entry in the MAC address table. The switch forwards packets with the specified source or destination MAC address. Only unicast static addresses are supported. By default, this command is disabled.

Use the no form of this command to reset it.

For procedures to configure and display the MAC addresses, see "Displaying and Setting MAC Addresses" on page 32.

Command Mode

Configuration Terminal mode

Example

The following example deletes the MAC address "000C.6E73.2BC4" on interface 4 on VLAN 9:

```
switch# configure terminal
switch#(config)# mac address-table static
000C.6E73.2BC4 discard interface ge4 vlan 9
```

Related Commands

“MAC ADDRESS-TABLE STATIC FORWARD” on page 141

“MAC ADDRESS-TABLE AGEING-TIME” on page 138

“SHOW MAC ADDRESS-TABLE” on page 92

MAC ADDRESS-TABLE STATIC FORWARD

Syntax

```
mac address-table static MAC forward interface IFNAME
vlan VLANID
```

```
no mac address-table static
```

Parameters

MAC	Indicates the static MAC address in the following format: MMM.MMM.MMM
IFNAME	Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with "ge."
VLANID	Indicates the VLAN interface. Enter a value between 2 and 4094. If you do not enter a value, VLAN 1 is assumed by default.

Description

The MAC ADDRESS-TABLE STATIC FORWARD command to create an entry in the MAC address table. The switch drops packets with the specified source or destination MAC address. Only unicast static addresses are supported. By default, this command is disabled. Use the no form of this command to reset it.

For procedures to configure and display the MAC addresses, see "Displaying and Setting MAC Addresses" on page 32.

Command Mode

Configuration Terminal mode

Example

The following example sets the MAC address of "000C.6E73.2BC4" on interface 3 and VLAN 2:

```
switch# configure terminal
switch#(config)# mac address-table static
000C.6E73.2BC4 forward interface ge3 vlan 2
```

Related Commands

“MAC ADDRESS-TABLE AGEING-TIME” on page 138

“MAC ADDRESS-TABLE STATIC DISCARD” on page 139

“SHOW MAC ADDRESS-TABLE” on page 92

MLS QOS

Syntax

```
mls qos <0-10> <0-7> | <0-10> <0-7> | <0-10> <0-7> |
<0-10> <0-7> | <0-10> <0-7> | <0-10> <0-7> | <0-10> <0-7> | <0-10> <0-7> |
```

Parameters

<0-10>	Specifies the weight for queue 0, where 0 indicates strict priority.
<0-7>	Specifies the priority for queue 0, where 0 indicates strict priority.
<0-10>	Specifies the weight for queue 1, where 0 indicates strict priority.
<0-7>	Specifies the priority for queue 1, where 0 indicates strict priority.
<0-10>	Specifies the weight for queue 2, where 0 indicates strict priority.
<0-7>	Specifies the priority for queue 2, where 0 indicates strict priority.
<0-10>	Specifies the weight for queue 3, where 0 indicates strict priority.
<0-7>	Specifies the priority for queue 3, where 0 indicates strict priority.
<0-10>	Specifies the weight for queue 4, where 0 indicates strict priority.
<0-7>	Specifies the priority for queue 4, where 0 indicates strict priority.
<0-10>	Specifies the weight for queue 5, where 0 indicates strict priority.
<0-7>	Specifies the priority for queue 5, where 0 indicates strict priority.
<0-10>	Specifies the weight for queue 6, where 0 indicates strict priority.

- <0-7> Specifies the priority for queue 6, where 0 indicates strict priority.
- <0-10> Specifies the weight for queue 7, where 0 indicates strict priority.
- <0-7> Specifies the priority for queue 7, where 0 indicates strict priority.

Description

The MLS QOS command to define queues for the Quality of Service feature. This command configures the default queues for any packet arriving on the specified interface. You must configure all of the queues.

Use the no form of this command to turn off the use of a default queue.

Command Mode

Configuration Terminal mode

Example

The following example sets queue 0 with a weight of 10 and a priority of 7, queue 1 with a weight of 9 and a priority of 6, and the remaining queues with a weight of 1 and a priority of 1:

```
switch# configure terminal
switch#(config)# mls qos 10 7 9 6 1 1 1 1 1 1 1 1 1 1 1
1
```

Related Commands

“USER-PRIORITY” on page 193

NTP AUTHENTICATE

Syntax

```
ntp authenticate  
no ntp authenticate
```

Parameters

none

Description

Use the NTP AUTHENTICATE command to enable authentication of the Network Time Protocol (NTP) time source. By default, this command is disabled. To disable NTP authentication on the switch, use the no form of this command.

For procedures to configure NTP, see “Setting the Network Time” on page 29.

Command Mode

Configuration Terminal mode

Example

The following commands enable authentication of the NTP time source:

```
switch#configure terminal  
switch(config)#ntp authenticate
```

Related Commands

“CLOCK SUMMER-TIME RECURRING” on page 117

“CLOCK TIMEZONE” on page 119

“NTP TRUSTED-KEY” on page 150

NTP AUTHENTICATION-KEY

Syntax

```
ntp authentication-key KEYNUMBER <1-4294967295>  
md5 KEY
```

```
no ntp authentication-key KEYNUMBER <1-4294967295>
```

Parameters

KEYNUMBER Specifies a key number. Choose a value between 1 and 4,294,967,295. This key indicates a trusted time source.

MD5 Indicates MD5 (message digest algorithm 5) authentication.

KEY Specifies the name of an authentication key.

Description

Use the NTP AUTHENTICATION-KEY command to define an authentication key for a trusted time source. If you set this command, the AT-S100 software only synchronizes to a system that carries one of the authentication keys specified. By default, this command is disabled.

To remove an authentication key, use the no form of this command.

For procedures to configure NTP, see “Setting the Network Time” on page 29.

Command Mode

Configuration Terminal mode

Example

The following commands specify an authentication key of “888” and a key name of “topsecretkey.”

```
switch#configure terminal
```

```
switch(config)#ntp authentication-key 888 md5  
topsecretkey
```

Related Commands

"NTP AUTHENTICATE" on page 145

"NTP TRUSTED-KEY" on page 150

NTP SERVER

Syntax

```
ntp server WORD prefer|version <1-4>|key <1-4294967295>
```

Parameters

WORD	Indicates the IP address of the NTP server. Use the following format: xxx.xxx.xxx.xxx
prefer	Specifies the software prefers this peer when possible.
version	Indicates the NTP version. Specify versions 1 through 4.
key	Indicates the peer key number that permits access to the specified NTP server.

Description

Use the NTP SERVER command to specify the IP address of the NTP server, a key to access the server, and the NTP version number. In addition, you can specify if the software prefers this NTP server over other NTP servers.

Note

To add more than one NTP server to the switch, enter a second NTP SERVER command with another IP address.

For procedures to configure NTP, see “Setting the Network Time” on page 29.

Command Mode

Configuration Terminal mode

Example

The following example sets the IP address of the NTP server to 198.11.1.9 and shows the resulting display:

```
switch#configure terminal
```

```
switch(config)#ntp server 198.11.1.9
```

```
Translating "198.11.1.9"... [OK]
```

Related Commands

"NTP AUTHENTICATE" on page 145

"NTP AUTHENTICATION-KEY" on page 146

"NTP TRUSTED-KEY" on page 150

NTP TRUSTED-KEY

Syntax

```
ntp trusted-key <1-4294967295>  
no ntp trusted-key <1-4294967295>
```

Parameters

none

Description

Use the NTP TRUSTED-KEY command to specify a key number for a trusted time source. You must first define a key number with the NTP AUTHENTICATION-KEY command. Enter a value between 1 and 4294967295.

By default, no trusted keys are defined. To disable the authentication of a device, use the no form of this command.

For procedures to configure NTP, see “Setting the Network Time” on page 29.

Command Mode

Configuration Terminal mode

Example

The following commands set the trusted key to 222,222:

```
switch#configure terminal  
switch(config)#ntp trusted-key 222222
```

Related Commands

“NTP AUTHENTICATE” on page 145

“NTP AUTHENTICATION-KEY” on page 146

“NTP SERVER” on page 148

SHOW LIST

Syntax

`show list`

Parameters

none

Description

Use the SHOW LIST command to display a list of all the commands available in the current mode.

The display of the SHOW LIST command is often more than one page. To advance the display to the next line, press ENTER. To advance the display to the next page, press ESC.

Command Mode

All modes

Example

Use the following commands to display the commands available in the current mode:

```
switch#configure terminal
```

```
switch#show list
```

See Figure 14 on page 152 for a sample display of the SHOW LIST command in the Privileged Executive mode.

```
(switch3)#show list
boot config-file WORD
cat WORD
clear arp-cache
clear counters IFNAME
clear gmrp statistics all
clear gmrp statistics vlanid <1-4094>
clear gvrp statistics IFNAME
clear gvrp statistics all
clear gvrp statistics all
clear ipmg
clear ipmg group *
clear ipmg group A.B.C.D
clear ipmg group A.B.C.D IFNAME
--More--
```

Figure 14. SHOW LIST Command

Related Commands

“SHOW RUNNING-CONFIG” on page 153

“SHOW RUNNING-CONFIG COMMUNITY-LIST” on page 158

“SHOW RUNNING-CONFIG INTERFACE” on page 160

SHOW RUNNING-CONFIG

Syntax

`show running-config`

Parameters

none

Description

Use the SHOW RUNNING-CONFIG command to display information about the system.

The display of the RUNNING-CONFIG command is often more than one page. To advance the display to the next line, press ENTER. To advance the display to the next page, press ESC.

Command Mode

All modes

Example

The following is an example of the SHOW RUNNING-CONFIG command and a sample of the output:

```
switch#show running-config
```

This command displays a variety of switch parameters. An example of page 1 of the display is shown in Figure 15.

```
(switch3)(config)# show running-config
!
no service password-encryption
!
log file system max-file-size 4096 level 7
username manager privilege 15 password friend
username operator password operator
!
snmp-server enable
!
ip multicast-routing
!
spanning-tree mode rstp
spanning-tree acquire
!
!
interface ge1
switchportaccess vlan 3
interface ge2
traffic-class-table user-priority 7 num-traffic-classes 2 value 0
interface ge3
switchport mode trunk
switchport trunk allowed vlan add 3
--More--
```

Figure 15. SHOW RUNNING-CONFIG Command, page 1

See Figure 16 for page 2 of the SHOW RUNNING-CONFIG command display.

```
interface ge4
static-channel-groups
interface ge5
static-channel-group4
interface ge6
user-priority 7
interface ge7
mtu 1518
interface ge8
!
interface ge9
!
interface ge10
!
!interface ge11
!
interface ge12
!
interface ge13
!
interface ge14
--More--
```

Figure 16. SHOW RUNNING-CONFIG Command, page 2

See Figure 17 for page 3 of the SHOW RUNNING-CONFIG command display.

```
interface ge15
!  
interface ge16
!  
interface ge17
!  
interface ge18
!  
interface ge19
!  
interface ge20
!  
interface ge21
!  
!interface ge22
!  
interface ge23
!  
interface ge24
!  
interface ge25
--More--
```

Figure 17. SHOW RUNNING-CONFIG Command, page 3

See Figure 18 for page 4 of the SHOW RUNNING-CONFIG command display.

```
interface ge26
!
interface ge27
!
interface lo
  ip address 127.0.0.1/8
  shutdown
!
interface vlan1
  ip address 192.10.4.110/8
!
no snmp-server enable trap snmp auth
no spanning-tree rstp enable forward
!
clock summer-time PDT recurring 2 sun mar 02:00 1 sun nov 02:00
line con 0
  login local
line vty 0 4
  login local
!
end
--More--
```

Figure 18. SHOW RUNNING-CONFIG Command, page 4

Related Commands

“SHOW LIST” on page 151

“SHOW RUNNING-CONFIG COMMUNITY-LIST” on page 158

“SHOW RUNNING-CONFIG INTERFACE” on page 160

SHOW RUNNING-CONFIG COMMUNITY-LIST

Syntax

```
show running-config community-list
```

Parameters

```
show running-config ip igmp snooping (> WORD) |  
(|begin|exclude|include|redirect LINE)
```

Parameters

- | | |
|----------|--|
| > | Indicates the output redirection. Specify the following: |
| WORD | Indicates the name of the file that the output is redirected to. |
| | Indicates the output redirection. Specify the following: |
| begin | Indicates to begin with a line that matches. |
| exclude | Specifies to exclude lines that match. |
| include | Indicates to include lines that match. |
| redirect | Indicates to redirect output. |
| LINE | Specifies a regular expression. |

Description

Use the SHOW RUNNING-CONFIG COMMUNITY-LIST command to display information about an SNMP community.

Command Mode

All modes

Example

The following is an example of the SHOW RUNNING-CONFIG COMMUNITY-LIST command:

```
switch#show running-config community-list
```

Related Commands

“SHOW RUNNING-CONFIG” on page 153

“SNMP-SERVER VIEW” on page 241

SHOW RUNNING-CONFIG INTERFACE

Syntax

```
show running-config interface INTERFACE
```

Parameters

IFNAME Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with “ge.”

Note

Do not mix interface types in a list. Also, the specified interfaces must exist.

Description

Use the SHOW RUNNING-CONFIG INTERFACE command to display the current configuration of one or more interfaces on the device.

Command Mode

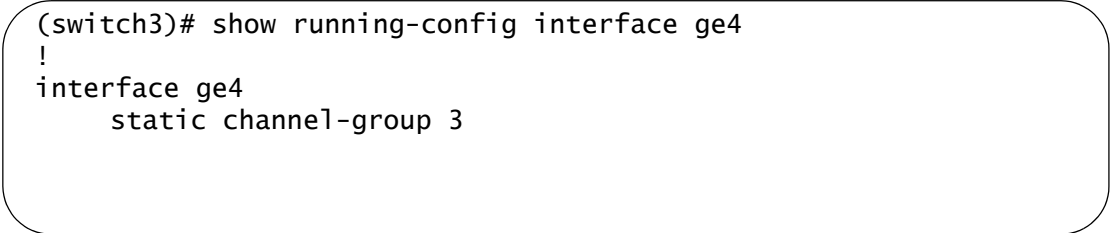
All modes

Examples

To display the status of the SHOW RUNNING-CONFIG INTERFACE command on port 4:

```
switch#show running-config interface ge4
```

See Figure 19 for an example display.



```
(switch3)# show running-config interface ge4
!
interface ge4
    static channel-group 3
```

Figure 19. SHOW RUNNING-CONFIG INTERFACE Port Example

To display the status of the current running configuration of a switch for VLAN 1:

```
switch#show running-config interface vlan1
```


See Figure 19 for an example display.

```
(switch3)# show running-config interface vlan2
!  
interface vlan1  
  ip address 192.10.8.1
```

Figure 20. SHOW RUNNING-CONFIG INTERFACE VLAN Example

Related Commands

“SHOW RUNNING-CONFIG” on page 153

USERNAME

Syntax

```
username WORD privilege <1-15> password LINE <8>
```

Parameters

WORD	Specifies a user name.
privilege	Specifies a user privilege level. Enter a value between 1 and 15. Values 1 through 14 provide operator privileges. Value 15 provides an administrator, or manager, privileges.
LINE	Specifies a password for an administrator or manager. Enter an alphanumeric value between 1 and 8 characters in length.

Description

Use the USERNAME command to set a user name, password, and privilege level. By default, the AT-S100 software provides one USERNAME type named “manager.”

A manager login has permission to perform all of the AT-S100 software commands in all of the command modes.

Command Modes

Configuration Terminal mode

Examples

The following command sets the user name to “jenny,” the privilege to “15,” and the password to “friend:”

```
switch#configure terminal
```

```
switch(config)#username jenny privilege 15 password  
friend
```

Related Commands

“ENABLE PASSWORD” on page 124

Chapter 5

Interface Configuration Mode Commands

This chapter provides descriptions of the commands in the Interface Configuration mode which can access either a port or a vlan interface. For more information about this mode, see “Interface Configuration Command Mode” on page 20.

This chapter describes the following commands:

- ❑ “CHANNEL-GROUP” on page 165
- ❑ “DOT1X PORT-CONTROL” on page 166
- ❑ “EXIT” on page 167
- ❑ “FLOW CONTROL BACKPRESSURE” on page 168
- ❑ “FLOW CONTROL RECEIVE” on page 169
- ❑ “FLOW CONTROL SEND” on page 170
- ❑ “IP ADDRESS” on page 171
- ❑ “IP ADDRESS DHCP” on page 173
- ❑ “LACP SYSTEM-PRIORITY” on page 174
- ❑ “MDIX” on page 175
- ❑ “MIRROR INTERFACE DIRECTION” on page 176
- ❑ “MTU” on page 178
- ❑ “SHOW RUNNING-CONFIG INTERFACE” on page 179
- ❑ “SHUTDOWN” on page 181
- ❑ “SPEED” on page 182
- ❑ “STATIC-CHANNEL-GROUP” on page 184
- ❑ “STORM-CONTROL” on page 185
- ❑ “SWITCHPORT ACCESS VLAN” on page 187
- ❑ “SWITCHPORT MODE TRUNK” on page 188
- ❑ “SWITCHPORT TRUNK ALLOWED VLAN” on page 190
- ❑ “TRAFFIC-CLASS-TABLE USER-PRIORITY NUM-TRAFFIC-CLASSES” on page 192
- ❑ “USER-PRIORITY” on page 193

Note

For information about the port security commands which are also in the Interface Configuration mode, see Chapter 8, “Port Security Commands” on page 219.

CHANNEL-GROUP

Syntax

```
channel-group <1-10> mode active|passive
no channel-group
```

Parameters

<1-10>	Specifies a channel group. Enter a value between 1 and 10.
mode	Specifies the status of LACP negotiation on a port. Choose from the following:
active	Enables initiation of LACP negotiation on a port.
passive	Disables initiation of LACP negotiation on a port.

Description

Use the CHANNEL-GROUP command to create a channel-group and enable or disable LACP negotiation on a port. To remove a channel group from an interface, use the no form of this command.

Command Mode

Interface Configuration mode

Example

The following commands create channel group 3 and make it active on interface 20:

```
switch# configure terminal
switch(config)# interface ge20
switch(config-if)# channel-group 3 active
```

Related Commands

“SHOW RUNNING-CONFIG” on page 153

“SHOW STATIC-CHANNEL-GROUP” on page 109

DOT1X PORT-CONTROL

Syntax

```
dot1x port-control auto|force-authorized|force-unauthorized dir=both|in
```

```
no dot1x port-control
```

Parameters

force-authorized	Forces an interface to an authorized state.				
force-unauthorized	Forces an interface to an unauthorized state.				
auto	Allows a client to negotiate authentication on an interface.				
dir	Specifies the packet control direction, where: <table><tr><td>both</td><td>Discards receive and transmit packets from the supplicant.</td></tr><tr><td>in</td><td>Discards receive packets from the supplicant.</td></tr></table>	both	Discards receive and transmit packets from the supplicant.	in	Discards receive packets from the supplicant.
both	Discards receive and transmit packets from the supplicant.				
in	Discards receive packets from the supplicant.				

Description

Use the DOT1X PORT-CONTROL command to force a port state on an interface. To remove an interface from the 802.1x management, use the no form of this command.

Command Mode

Interface mode

Example

The following commands enable authentication on interface 20:

```
switch# configure terminal
switch(config)# interface ge20
switch(config-if)# dot1x port-control auto
```

Related Commands

none

EXIT

Syntax

`exit`

Parameters

none

Description

Use the EXIT command to quit the Configuration Terminal mode and enter the Privileged Executive mode. After you enter this command, the prompt changes to “Switchname#” to indicate the Privileged Executive mode.

Command Mode

Configuration Terminal mode

Example

The following commands exit the Configuration Terminal mode and returns the software to the Privileged Executive mode:

```
switch#configure terminal
```

```
switch(config)#exit
```

```
switch#
```

Related Commands

none

FLOW CONTROL BACKPRESSURE

Syntax

```
flow control backpressure on|off
```

Parameters

backpressure Specifies back-pressure flow-control in half-duplex mode. Choose from the following options.

on Enables back pressure.

off Disables back pressure.

Description

Use the FLOWCONTROL BACKPRESSURE command to enable or disable back-pressure flow-control on an interface.

Command Mode

Interface Configuration mode

Example

The following commands turn on back-pressure flow-control in half-duplex mode on port 4:

```
switch#configure terminal
```

```
switch(config)#interface ge4
```

```
switch(config-if)#flowcontrol backpressure on
```

Related Commands

“FLOW CONTROL SEND” on page 170

“FLOW CONTROL RECEIVE” on page 169

FLOW CONTROL RECEIVE

Syntax

```
flow control receive on|off
```

Parameters

receive Controls flow control on traffic that is received by an interface. Choose from the following options:

on Enables flow control.

off Disables flow control.

Description

Use the FLOWCONTROL RECEIVE command to enable an interface to receive traffic using flow control.

Flow control enables connected Ethernet ports (or interfaces) to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies another port to stop sending traffic until the condition clears. When the local device detects congestion at its end, it notifies the remote device by sending a pause frame. After the remote device receives a pause frame, the remote device stops sending data packets. This prevents the loss of data packets during the congestion period.

Command Mode

Interface Configuration mode

Example

The following commands set port 7 to flow control receive on.

```
switch#configure terminal
```

```
switch(config)#interface ge7
```

```
switch(config-if)#flow control receive on
```

Related Commands

“FLOW CONTROL BACKPRESSURE” on page 168

“FLOW CONTROL SEND” on page 170

FLOW CONTROL SEND

Syntax

```
flow control send on|off
```

Parameters

send Controls flow control on traffic that is sent by an interface. Choose from the following options:

on Enables flow control.

off Disables flow control.

Description

Use the FLOWCONTROL SEND command to enable an interface to send traffic using flow control.

Flow control enables connected Ethernet ports (or interfaces) to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies another port to stop sending traffic until the condition clears. When the local device detects congestion at its end, it notifies the remote device by sending a pause frame. After the remote device receives a pause frame, the remote device stops sending data packets. This prevents the loss of data packets during the congestion period.

Command Mode

Interface Configuration mode

Example

The following commands set port 20 to flow control send on.

```
switch#configure terminal
```

```
switch(config)#interface ge20
```

```
switch(config-if)#flow control send on
```

Related Commands

“FLOW CONTROL BACKPRESSURE” on page 168

“FLOW CONTROL RECEIVE” on page 169

IP ADDRESS

Syntax

```
ip address A.B.C.D/M label LABEL secondary
```

Parameters

A.B.C.D/M	Specifies the IP address of the interface followed by a slash and a subnet mask.
LABEL	Specifies the label, or name, of the IP address.
secondary	Indicates that this IP address is a secondary IP address.

Description

Use the IP ADDRESS command to assign an IP address to a VLAN interface and label the address. In addition, this command assigns the IP address as either a primary or a secondary IP address for the specified interface.

You must configure the primary IP address before the secondary IP address. Also, the secondary IP address cannot be the same address as the primary IP address.

You must assign an IP address to a VLAN in the Interface Command Mode. You may assign the IP address to the default VLAN which is VLAN 1 or to a VLAN that you have created. For information about how to create a VLAN, see "Creating VLANs" on page 40.

Command Mode

Interface Configuration mode

Examples

The following commands set VLAN 1 with the primary IP address of 10.0.0.1 and a subnet mask of 255.255.255.255.0 (24 bits) and labels the IP address as "englab5."

```
switch#configure terminal
switch(config)#interface vlan1
switch(config-if)#ip address 10.0.0.1/8 label englab5
```

The following commands set VLAN 2 with the secondary IP address and mask of 192.10.0.5/8 and labels the IP address as “Sales2” to VLAN2:

```
switch#configure terminal
```

```
switch(config)#interface vlan2
```

```
switch(config-if)#ip address 192.10.0.5/8 label sales2  
secondary
```

Related Commands

“IP ADDRESS DHCP” on page 173

“SHOW RUNNING-CONFIG” on page 153

“VLAN” on page 267

IP ADDRESS DHCP

Syntax

`ip address DHCP`

Parameters

DHCP Indicates the DHCP client is used to obtain an IP address for this interface.

Description

Use the IP ADDRESS DHCP command to allow an DHCP server to assign an IP address to an interface. You can enable DHCP on a port or on a VLAN.

Command Mode

Interface Configuration mode

Examples

The following commands set VLAN 1 with an IP address obtained by the DHCP server:

```
switch#configure terminal
switch(config)#interface vlan1
switch(config-if)#ip address dhcp
```

The following commands set port 4 with an IP address obtained by the DHCP server:

```
switch#configure terminal
switch(config)#interface ge4
switch(config-if)#ip address dhcp
```

Related Commands

“IP ADDRESS” on page 171

“SHOW RUNNING-CONFIG” on page 153

LACP SYSTEM-PRIORITY

Syntax

```
lacp system-priority <1-65535>
```

```
no lacp system-priority
```

Parameters

<1-65535> Specifies the LACP port priority. Lower numerical values have higher priorities.

Description

Use the LACP SYSTEM-PRIORITY command to set the system priority of a local system. This is used in determining the system responsible for resolving conflicts in the choice of aggregation groups. The default value is 32,768.

Use the no form of this command to reset the priority of the switch to the default value.

Command Mode

Interface Configuration mode

Example

The following commands set the switch with an LACP priority of 6700:

```
switch#configure terminal
```

```
switch(config)#lacp system-priority 6700
```

Related Commands

none

MDIX

Syntax

```
mdix mdi|mdix
```

Parameters

mdi Specifies the interface is forced to MDI mode.

mdix Specifies the interface is forced to MDIX mode.

Description

Use the MDIX command to force an interface to the MDI or MDIX mode. This command only applies to copper ports 1-24 on the AT-9000/28 switch. The MDIX command does not apply to fiber ports.

Command Mode

Interface Configuration mode

Example

The following commands force interface 7 to MDI mode:

```
switch#configure terminal
switch(config)#interface ge7
switch(config-if)#mdix mdi
```

Related Commands

“SPEED” on page 182

MIRROR INTERFACE DIRECTION

Syntax

```
mirror interface ge<1-28> direction  
both|receive|transmit
```

```
no mirror interface ge<1-28> direction  
both|receive|transmit
```

Parameters

interface	Specifies the port-mirroring-destination port on the switch.
direction	Specifies the interface is forced to MDIX mode. Choose from the following options: <ul style="list-style-type: none">both Mirror traffic in both directions.receive Mirror received traffic.transmit Mirror transmitted traffic.

Description

Use the MIRROR INTERFACE DIRECTION command to create a port mirror and specify the direction of the port mirroring. You can only specify one active port at a time.

To turn off port mirroring, use the no command.

Command Mode

Interface mode

Examples

The following commands set port 19 to receive port mirroring traffic from port 20:

```
switch#configure terminal
```

```
switch(config)#interface ge20
```

```
switch(config-if)#mirror interface ge19 direction  
receive
```


The following commands turn off port mirroring on port 20:

```
switch#configure terminal
```

```
switch(config)#interface ge20
```

```
switch(config-if)#no mirror interface ge19 direction  
receive
```

Related Commands

“SHOW RUNNING-CONFIG” on page 153

MTU

Syntax

```
mtu <64-9216>
```

Parameters

none

Description

Use the MTU command to set the MTU value for the specified interface. Choose a value between 64 and 9,216.

Command Mode

Interface mode

Example

The following commands set port 22 with an MTU value of 1700:

```
switch#configure terminal
switch(config)#interface ge22
switch(config-if)#mtu 1700
```

Related Commands

“SHOW RUNNING-CONFIG INTERFACE” on page 179

SHOW RUNNING-CONFIG INTERFACE

Syntax

```
show running-config interface INTERFACE
```

Parameters

INTERFACE Indicates the interface or a list of interfaces. An interface list can consist of a port.

Note

Do not mix interface types in a list. Also, the specified interfaces must exist.

Description

Use the SHOW RUNNING-CONFIG INTERFACE command to display the current configuration of one or more interfaces on the device.

Command Mode

All modes

Examples

To display the status of the SHOW RUNNING-CONFIG INTERFACE command on port 4:

```
switch#show running-config interface ge4
```

See Figure 21 for an example display.

```
(switch3)# show running-config interface ge4
!
interface ge4
    static channel-group 3
```

Figure 21. SHOW RUNNING-CONFIG INTERFACE Port Example

To display the status of the current running configuration of a switch for VLAN 2:

```
switch#show running-config interface vlan2
```

See Figure 21 for an example display.

```
(switch3)# show running-config interface vlan2
!  
interface vlan2  
!
```

Figure 22. SHOW RUNNING-CONFIG INTERFACE VLAN Example

Related Commands

“SHOW RUNNING-CONFIG” on page 153

SHUTDOWN

Syntax

shutdown

no shutdown

Parameters

none

Description

Use the SHUTDOWN command to shut down the specified interface.

Use the no form of this command to restore or reactivate a connection with the specified interface.

Command Mode

Interface Configuration mode

Example

The following commands shutdown port 23:

```
switch#configure terminal
```

```
switch(config)#interface ge23
```

```
switch(config-if)#shutdown
```

Related Commands

none

SPEED

Syntax

```
speed
10000mfull | 1000mfull | 100mfull | 100mhalf | 100fx | 10mfull |
10mhalf | auto

no speed
```

Parameters

10000mfull	Specifies the interface is forced to operate at a speed of 10,000 Mbps in full duplex mode.
1000mfull	Specifies the interface is forced to operate at a speed of 1,000 Mbps in full duplex mode.
100mfull	Specifies the interface is forced to operate at a speed of 100 Mbps in full duplex mode.
100mhalf	Specifies the interface is forced to operate at a speed of 100 Mbps in half duplex mode.
100fx	Specifies the interface is forced to operate at a speed of 100FX on an uplink port that is connected to an SFP transceiver. This setting applies to ports 25 through 28 on the AT-9000/28 switch. On the AT-9000/28SP switch, this setting applies to all of the ports. This speed is available in full-duplex mode only.
10mfull	Specifies the interface is forced to operate at a speed of 10 Mbps in full duplex mode.
10mhalf	Specifies the interface is forced to operate at a speed of 10 Mbps in half duplex mode.
auto	Enables auto speed and duplex configuration.

Description

Use the SPEED command to set the speed and duplex mode for each port on the switch. For ports ge24 through ge28, you need to manually set the port speed to 100FX when you insert an SFP.

Use the no form of this command to remove the interface speed.

Note

To display the current port speeds, use the SHOW INTERFACE command. See “SHOW INTERFACE” on page 90.

Note

For more information about the AT-9000 switches and their ports, see the *AT-9000 Managed Layer 2 GE ecoSwitch Family Installation Guide*.

Command Mode

Interface Configuration mode

Examples

The following commands set port 5 to 1,000Mbps in full-duplex mode:

```
switch#configure terminal
switch(config)#interface ge5
switch(config-if)#speed 1000mfull
```

The following commands set port 24 to 100FX in full-duplex mode on the AT-9000/28 switch:

```
switch#configure terminal
switch(config)#interface ge24
switch(config-if)#speed 100fx
```

The following commands set port 13 to 100FX in full-duplex mode on the AT-9000/28SP switch:

```
switch#configure terminal
switch(config)#interface ge13
switch(config-if)#speed 100fx
```

Related Commands

“SHOW INTERFACE” on page 90

STATIC-CHANNEL-GROUP

Syntax

```
static-channel-group <1-8>
```

```
no static-channel-group
```

Parameters

<1-8> Specifies the static-channel-group number.

Description

Use the STATIC-CHANNEL-GROUP command to create a static-channel group.

Use the no form of this command to remove a static-channel group.

Command Mode

Interface Configuration mode

Example

The following commands create channel group 2 on port 8:

```
switch#configure terminal
```

```
switch(config)#interface ge8
```

```
switch(config-if)#static-channel-group 2
```

Related Commands

“SHOW STATIC-CHANNEL-GROUP” on page 109

STORM-CONTROL

Syntax

```
storm-control broadcast|dlf|multicast LEVEL <1-100>
no storm-control broadcast|dlf|multicast
```

Parameters

broadcast	Sets the broadcast rate limiting value for the interface.
dlf	Sets the destination lookup failure (DLF) for the interface.
multicast	Sets the multicast rate limiting value for the interface.
LEVEL	Specifies the percentage of the threshold or the percentage of the maximum speed (pps) of the interface. Enter a value between 1 and 100.

Description

Flooding techniques are used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on an interface. Forwarding these packets can cause the network to slow down or timeout.

Use the STORM-CONTROL command to specify the rising threshold level for broadcasting, multicast, or destination-lookup-failure traffic. The storm control action occurs when traffic reaches the level specified with the LEVEL parameter. By default, storm control is disabled.

Use the no form of this command to disable storm control.

Command Mode

Interface Configuration mode

Example

The following commands set the broadcast rate to 30% on port 4:

```
switch#configure terminal
switch(config)#interface ge4
switch(config-if)#storm-control broadcast level 30
```

Related Commands

none

SWITCHPORT ACCESS VLAN

Syntax

```
switchport access vlan VLANID <2-4094>
```

```
no switchport access vlan VLANID <2-4094>
```

Parameters

VLANID Specifies a VLAN ID. Enter a value from 2 to 4094.

Description

Use the SWITCHPORT ACCESS VLAN command to change the default VLAN for an interface. By default, all ports are assigned to VLAN 1. Use the no form of this command to remove a previously created VLAN with the specified VLAN ID.



Caution

Before you enter the SWITCHPORT ACCESS VLAN command, you must configure a VLAN using the VLAN command.

Note

The default VLAN ID is 1. Do not use a VLAN ID of 1 due to interoperability issues.

Command Mode

Interface Configuration mode

Example

The following commands set the default VLAN to 3 on port 6:

```
switch#configure terminal
```

```
switch(config)#interface ge6
```

```
switch(config-if)#switchport access vlan 3
```

Related Commands

“SHOW VLAN ALL” on page 258

SWITCHPORT MODE TRUNK

Syntax

```
switchport mode trunk ingress-filter enable|disable  
no switchport mode
```

Parameters

ingress-filter	Sets the ingress filtering for the received frames. Choose from the following options:
enable	Sets the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.
disable	Turns off ingress filtering to accept frames that do not meet the classification criteria. This is the default value.

Description

Use the SWITCHPORT MODE TRUNK command to set the switching characteristics of the Layer-2 interface to trunk mode and specify tagged frames only. Received frames are classified based on the VLAN characteristics. Then they are accepted or discarded based on the specified filtering criteria.

Use the no form of this command to reset the mode of the Layer-2 interface to the default value which is ingress filtering is off and all frame types are classified and accepted.

Command Mode

Interface mode

Example

The following commands enable ingress filtering for received frames:

```
switch#configure terminal  
switch(config)#interface ge5  
switch(config-if)#switchport mode trunk ingress-filter  
enable
```

Related Commands

none

SWITCHPORT TRUNK ALLOWED VLAN

Syntax

```
switchport trunk allowed vlan add|remove VLANID  
no switchport trunk vlan
```

Parameters

- | | |
|--------|---|
| add | Add a VLAN to transmit and receive through the Layer-2 interface. |
| remove | Remove a VLAN that transmits and receives through the Layer-2 interface. |
| VLANID | Specifies a VLAN ID or a list of VLAN IDs. Enter a value from 2 to 4094. Set a single VLAN, VLAN range, or a VLAN list.

For a VLAN range, specify the lowest VLAN, then the highest VLAN number in the range, and separate them with a hyphen.

For a VLAN list, specify VLAN numbers separated by commas. |

Note

Do not enter spaces between hyphens or commas when setting parameters for VLAN ranges or lists.

Description

Use the SWITCHPORT TRUNK ALLOWED VLAN command to change the default VLAN for an interface. Use the no form of this command to remove a previously created VLAN with the specified VLAN ID.

Command Mode

Interface Configuration mode

Examples

The following commands add a single VLAN, VLAN 2, to the member set of port 6:

```
switch#configure terminal  
switch(config)#interface ge6
```

```
switch(config-if)#switchport mode trunk
```

```
switch(config-if)#switchport trunk allowed vlan add 2
```

The following commands add VLANs 2 through 6 to the member set of port 7:

```
switch#configure terminal
```

```
switch(config)#interface ge7
```

```
switch(config-if)#switchport mode trunk
```

```
switch(config-if)#switchport trunk allowed vlan add 2-6
```

The following commands remove a list of VLANs from port 5:

```
switch#configure terminal
```

```
switch(config)#interface ge5
```

```
switch(config-if)#switchport mode trunk
```

```
switch(config-if)#switchport trunk allowed vlan remove
```

Related Commands

“SHOW VLAN ALL” on page 258

“SWITCHPORT MODE TRUNK” on page 188

TRAFFIC-CLASS-TABLE USER-PRIORITY NUM-TRAFFIC-CLASSES

Syntax

```
traffic-class-table user-priority <0-7> num-traffic-classes <0-8> value <0-2?>
```

Parameters

user-priority	Indicates the user priority associated with the traffic class table. Choose a value between 0 and 7.
num-traffic-classes	Indicates the number of supported traffic classes. Choose a value between 0 and 8.
value	Indicates the value that is used for the given user-priority and num-traffic classes.

Description

Use the TRAFFIC-CLASS-TABLE USER-PRIORITY NUM-TRAFFIC-CLASSES command to specify how the incoming 802.1p priority market packets are mapped to the internal Class of Service queues. Also, it allows you to display the number of queues per port.

To display the current port security settings, use the “SHOW RUNNING-CONFIG INTERFACE” on page 160.

Command Mode

Interface Configuration mode

Example

The following commands set port 3 with a user priority of 7, a traffic class value of 7, and a value of 2:

```
switch#configure terminal
switch(config)#interface ge3
switch(config-if)#traffic-class-table user-priority 7
num-traffic classes 7 value 2
```

Related Commands

none

USER-PRIORITY

Syntax

`user-priority <0-7>`

Parameters

none

Description

Use the USER-PRIORITY command to indicate a priority for the port specified.

A tagged Ethernet frame contains a field that specifies its VLAN membership. Such frames also contain a user priority level used by the switch to determine the Quality of Service to apply to the frame and which egress queue on the egress port a packet should be stored in. The three bit binary number represents eight priority levels, 0 to 7, with 0 the lowest priority and 7 the highest. By default, this command is set to 0 on all ports.

Command Mode

Interface mode

Example

The following commands assign a user priority of 7 to port 16:

```
switch#configure terminal
switch(config)#interface ge16
switch(config-if)#user-priority 7
```

Related Commands

“MLS QOS” on page 143

“USERNAME” on page 162

Section II

Advanced Configuration

The chapters in this section provide information about configuring advanced features:

- ❑ Chapter 6, “802.1x Access Control Commands” on page 197
- ❑ Chapter 7, “GVRP Commands” on page 211
- ❑ Chapter 8, “Port Security Commands” on page 219
- ❑ Chapter 9, “Simple Network Management Protocol (SNMP) Commands” on page 227
- ❑ Chapter 10, “Spanning Tree Protocol (STP) Commands” on page 243
- ❑ Chapter 11, “Virtual Local Area Networks (VLAN) Commands” on page 257

Chapter 6

802.1x Access Control Commands

The switch implements the server side of the IEEE 802.1x Port-based and MAC-based Network Access Control. This feature allows only authorized users, or their network devices, access to network resources by establishing criteria for each interface on the switch.

This chapter contains the following commands:

- ❑ “DOT1X PORT-CONTROL” on page 198
- ❑ “DOT1X SYSTEM-AUTH-CTRL” on page 199
- ❑ “LOGIN REMOTELOCAL” on page 200
- ❑ “RADIUS-SERVER HOST” on page 201
- ❑ “RADIUS-SERVER KEY” on page 202
- ❑ “SHOW DOT1X” on page 203
- ❑ “SHOW DOT1X ALL” on page 204
- ❑ “SHOW DOT1X INTERFACE” on page 207
- ❑ “SHOW DOT1X STATISTICS INTERFACE” on page 209

DOT1X PORT-CONTROL

Syntax

```
dot1x port-control auto|force-authorized|force-
unauthorized dir=both|in
```

```
no dot1x port-control
```

Parameters

force-authorized	Forces an interface to an authorized state.				
force-unauthorized	Forces an interface to an unauthorized state.				
auto	Allows a client to negotiate authentication on an interface.				
dir	Specifies the packet control direction, where: <table data-bbox="760 892 1430 1060"> <tr> <td>both</td><td>Discards receive and transmit packets from the supplicant.</td></tr> <tr> <td>in</td><td>Discards receive packets from the supplicant.</td></tr> </table>	both	Discards receive and transmit packets from the supplicant.	in	Discards receive packets from the supplicant.
both	Discards receive and transmit packets from the supplicant.				
in	Discards receive packets from the supplicant.				

Description

Use the DOT1X PORT-CONTROL command to force a port state on an interface. To remove an interface from the 802.1x management, use the no form of this command.

Command Mode

Interface mode

Example

The following commands enable authentication on interface 20:

```
switch# configure terminal
switch(config)# interface ge20
switch(config-if)# dot1x port-control auto
```

Related Commands

none

DOT1X SYSTEM-AUTH-CTRL

Syntax

```
dot1x system-auth-ctrl
```

Parameters

system-auth-ctrl Enable global interface authentication.

Description

Use the DOT1X SYSTEM-AUTH-CTRL command to enable authentication globally on interfaces 1 through 28. Global authentication is disabled by default.

Command Mode

Configuration Terminal mode

Example

The following commands enable 802.1x Port Based Access Control on all interfaces:

```
switch#configure terminal
```

```
switch(config)#dot1x system-auth-ctrl
```

Related Commands

“SHOW DOT1X ALL” on page 204

LOGIN REMOTELOCAL

Syntax

```
login remotelocal
```

```
no login
```

Parameters

none

Description

Use the LOGIN REMOTELOCAL command to enable password checking on the RADIUS server. To disable password checking, use the no form of the command.

Command Mode

Line mode

Example

The following commands enable password checking on a RADIUS server with an IP address of 192.168.1.30 and a key of "ATI:"

```
switch# configure terminal
```

```
switch(config)# radius-server host 192.168.1.30 auth-  
port 1812
```

```
switch(config)# radius-server key ATI
```

```
switch(config)# line console 0
```

```
switch(config-line)# login remotelocal
```

Related Commands

"LINE CONSOLE" on page 135

"RADIUS-SERVER HOST" on page 201

"RADIUS-SERVER KEY" on page 202

RADIUS-SERVER HOST

Syntax

```
radius-server host HOSTNAME auth-port=port|ALL <1-1812>
```

```
no radius-server host
```

Parameters

hostname	Sets the radius server to an IP address in the following format: xxx.xxx.xxx
auth-port	Specifies the port number of the radius client. The default port number is 1812. The range is from 1 to 1812.

Description

Use the RADIUS-SERVER HOST command to set the RADIUS server host name and port.

Use the no form of this command to remove the defined host and port from the list of RADIUS servers. If you do not specify a value for the port, the default value of 1812 is used automatically.

Command Mode

Configure mode

Example

The following commands assign an IP address of 192.126.12.1 to the radius-server host:

```
switch# configure terminal
switch(config)# radius-server host 192.126.12.1
```

Related Commands

none

RADIUS-SERVER KEY

Syntax

`radius-server key KEY`

`no radius-server key KEY`

Parameters

KEY The secret key shared among the radius server and the 802.1x client. Special characters such as "*", "_", and "!" are permitted.

Description

Use the RADIUS-SERVER KEY command to set the shared secret key between a Radius server and a client. This command has no default value.

To erase the current value of the secret key, use the no form of this command.

Command Mode

Configure mode

Example

The following commands set the shared secret key to "ketzel24:"

```
switch# configure terminal
```

```
switch(config)# radius-server key ketzel24
```

Related Commands

"RADIUS-SERVER HOST" on page 201

SHOW DOT1X

Syntax

```
show dot1x
```

Parameters

none

Description

Use this command to display the status of the 802.1x feature on the switch.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token).

Command Mode

Privileged Executive mode

Example

The following example shows the SHOW DOT1X command and the resulting display:

```
switch#show dot1x
```

See Figure 23 for a sample display.

```
switch# show dot1x
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.ipinfusion.com.12103
% Next radius message id: 0
```

Figure 23. SHOW DOT1X Command

Related Commands

“SHOW DOT1X ALL” on page 204

“SHOW DOT1X INTERFACE” on page 207

SHOW DOT1X ALL

Syntax

```
show dot1x all
```

Parameters

none

Description

Use this command to display detailed 802.1x information about all of the interfaces. To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token).

Command Mode

Privileged Executive mode

Example

The following example shows the SHOW DOT1X ALL command and the resulting display in Figure 24:

```
switch# show dot1x all
```

```
(switch3)#show dot1x all
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.ipinfusion.com.12103
% Next radius message id: 0
% Dot1x info for interface eth1 - 3
% portEnabled: true - portControl: auto
% portStatus: unauthorized - currentId: 11
% reAuthenticate: disabled
% abort:F fail:F start:F timeout:F success:F
% PAE: state: connecting - portMode: auto
% PAE: reAuthCount: 2 - rxRespId: 0
% PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
% BE: state: idle - reqCount: 0 - idFromServer: 0
% BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2
% CD: adminControlledDirections: in - operControlledDirections: in
% CD: bridgeDetected: false
% KR: rxKey: false
% KT: keyAvailable: false - keyTxEnabled: false
```

Figure 24. SHOW DOT1X ALL Command

Table 7 provides a description of the parameters of the SHOW DOT1X ALL and SHOW DOT1X INTERFACE commands.

Table 7. SHOW DOT1X Parameter Description

Parameter	Description
portEnabled	Indicates the interface operational status (up-true/down-false).
portControl	Indicates the current control status of the port for 802.1x control.
portStatus	Indicates the 802.1x status of the port (authorized or unauthorized).
reAuthenticate	Indicates the status of reauthentication on an interface.
reAuthPeriod	Indicates the time period of reauthentication.
Supplicant PAE related global variables:	
abort	Indicates that authentication should be aborted when this variable is set to true.
fail	Indicates failed authentication attempt when this variable is set to false.
start	Indicates authentication should be started when this variable is set to true.
timeout	Indicates an authentication attempt timed out when this variable is set to true.
success	Indicates authentication is successful when this variable is set to true.
PAE: state Current 802.1x operational state of the interface	
mode	Indicates the mode is set to 802.1x.
reAuthMax	Indicates the maximum number of reauthentication attempts.
BE Backend Authentication state	
state	Indicates the status of the state machine.
reqCount	Indicates the number of requests sent to the server.
suppTimeout	Indicates the supplicant timeout period.
serverTimeout	Indicates the server timeout period.

Table 7. SHOW DOT1X Parameter Description (Continued)

Parameter	Description
maxReq	Specifies the maximum number of requests that can be sent.
CD	Specifies the Controlled Directions State machine.
adminControlledDirections	Indicates the administrative value (Both/In).
operControlledDirections	Indicates the operational Value (Both/In).
KR	Specifies the key receive state machine.
rxKey	Indicates true when EAPOL-Key message is received by supplicant or authenticator. Indicates false when a key is transmitted.
KT	Specifies the Key Transmit State machine.
keyAvailable	Indicates false when key has been transmitted by authenticator. Indicates true when a new key is available for key exchange.
keyTxEnabled	Indicates the key transmission status.

Related Commands

“SHOW DOT1X INTERFACE” on page 207

SHOW DOT1X INTERFACE

Syntax

```
show dot1x interface IFNAME
```

Parameters

IFNAME Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with "ge."

Description

Use this command to display the state of a particular interface.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token).

Command Mode

Privileged Executive mode

Example

The following command displays the state of interface 6.

```
switch# show dot1x interface ge6
```

See Figure 25 for a sample display.

```
(switch3)#show dot1x interface
% 802.1X info for interface xe6
% portEnabled: true - portControl: Force Unauthorized
% portStatus: Unauthorized - currentId: 2
% reAuthenticate: disabled
% reAuthPeriod: 3600
% abort:F fail:F start:F timeout:F success:F
% PAE: state: Force Unauthorized - portMode: Force Unauthorized
% PAE: reAuthCount: 1 - rxRespId: 0
% PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 0
BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2
CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: falseExample
```

Figure 25. SHOW DOT1X INTERFACE Command

See Table 7 on page 205 for a description of the command parameters shown in Figure 25 on page 207.

Related Commands

“SHOW DOT1X ALL” on page 204

SHOW DOT1X STATISTICS INTERFACE

Syntax

show dot1x statistics interface IFNAME ge<1-28>

Parameters

IFNAME Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with "ge."

Description

Use the SHOW DOT1X STATISTICS INTERFACE command to display the vital statistics of an interface.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token).

Command Mode

Privileged Executive mode

Example

The following command displays the statistics for interface 5:

```
switch# show dot1x statistics interface ge5
```

See Figure 26 for a sample display.

```
(switch3)#show dot1x interface
% Dot1x statistics for interface xe5 - 3
% EAPOL Frames Rx: 0 - EAPOL Frames Tx: 0
% EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
% EAP Rsp/Id Frames Rx: 0 - EAP Response Frames Rx: 0
% EAP Req/Id Frames Tx: 35 - EAP Request Frames Tx: 0
% Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
% EAPOL Last Frame Version Rx: 0 - EAPOL Last Frame Src:
0000.0000.0000
```

Figure 26. SHOW DOT1X INTERFACE Command

Related Commands

"SHOW DOT1X" on page 203

GVRP Commands

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information. The main purpose of GVRP is to allow switches to automatically discover some of the VLAN information that would otherwise need to be manually configured in each switch. This is helpful in networks where VLANs span more than one switch. Without GVRP, you must manually configure your switches to ensure that the various parts of a VLAN can communicate across the different switches. GVRP, which is an application of the Generic Attribute Registration Protocol (GARP), does this for you automatically.

This chapter contains the following commands:

- ❑ “SET GVRP” on page 212
- ❑ “SET GVRP APPLICANT” on page 213
- ❑ “SET GVRP DYNAMIC-VLAN-CREATION” on page 214
- ❑ “SET GVRP REGISTRATION” on page 215
- ❑ “SET GVRP TIMER” on page 217

Note

For information about VLAN commands, see Chapter 11, “Virtual Local Area Networks (VLAN) Commands” on page 257.

SET GVRP

Syntax

```
set gvrp enable|disable
```

Parameters

enable Enables GVRP on the switch.

disable Disables GVRP on the switch.

Description

This command enables or disables GVRP globally on the switch. When GVRP is enabled, the switch learns GVRP VLANs and GVRP ports dynamically.

When GVRP is disabled, the switch does not learn any new dynamic GVRP VLANs or dynamic GVRP ports.

Command Mode

Configuration Terminal mode

Examples

The following commands enable GVRP on the switch:

```
switch#configure terminal
```

```
switch(config)#set gvrp enable
```

The following commands disable GVRP on the switch:

```
switch#configure terminal
```

```
switch(config)#set gvrp disable
```

Related Commands

“SET GVRP APPLICANT” on page 213

“SET GVRP DYNAMIC-VLAN-CREATION” on page 214

“SET GVRP REGISTRATION” on page 215

“SET GVRP TIMER” on page 217

SET GVRP APPLICANT

Syntax

```
set gvrp applicant state active|normal ge<1-28>
```

Parameters

active	Indicates the active state. The port participates in GVRP. The port processes GVRP information and transmits PDUs.
normal	Indicates the normal state. The port does not participate in GVRP. The port neither processes GVRP information nor transmits PDUs.
ge<1-28>	Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with "ge."

Description

The GVRP APPLICANT command sets the GID applicant state on a port to active or normal.

Command Mode

Configuration Terminal mode

Examples

The following commands set the GID applicant on port 5 to an active state:

```
switch#configure terminal
switch(config)#set gvrp applicant state active ge5
```

Related Commands

"SET GVRP" on page 212

"SET GVRP DYNAMIC-VLAN-CREATION" on page 214

"SET GVRP REGISTRATION" on page 215

"SET GVRP TIMER" on page 217

SET GVRP DYNAMIC-VLAN-CREATION

Syntax

```
set gvrp dynamic-vlan-creation
```

Parameters

none

Description

The GVRP DYNAMIC-VLAN-CREATION command enables dynamic VLANs to be created on the switch.

Command Mode

Configuration Terminal mode

Example

The following commands allow GVRP VLANs to be created dynamically on the switch:

```
switch#configure terminal  
switch(config)#set gvrp dynamic-vlan-creation
```

Related Commands

“SET GVRP” on page 212

“SET GVRP APPLICANT” on page 213

“SET GVRP REGISTRATION” on page 215

“SET GVRP TIMER” on page 217

SET GVRP REGISTRATION

Syntax

```
set gvrp registration fixed|forbidden|normal ge<1-28>
```

Parameters

fixed	Allows manual creation and registration of VLANs and prevents VLAN deregistration. Also registers all known VLANs on other port on the tagged port.
forbidden	Unregisters all VLANs (except VLAN 1) and prevents any further VLAN creation or registration on the tagged port.
normal	Allows dynamic creation (if dynamic VLAN creation is enabled), registration, and deregistration of VLANs on the tagged port. This is the default value.
ge<1-28>	Specifies the name of an interface. There are 28 ports on the AT-9000/28 and AT-9000/28SP switches. To specify a port, precede the port number with "ge."

Description

Use the SET GVRP REGISTRATION command to set GVRP registration to fixed, forbidden, or normal on an interface.

Command Mode

Configuration Terminal mode

Examples

The following commands set GVRP registration to fixed on port 9:

```
switch#configure terminal
switch(config)#set gvrp registration fixed ge9
```

The following commands set GVRP registration to forbidden on port 15:

```
switch#configure terminal
switch(config)#set gvrp registration forbidden ge15
```

Related Commands

“SET GVRP” on page 212

“SET GVRP APPLICANT” on page 213

“SET GVRP DYNAMIC-VLAN-CREATION” on page 214

“SET GVRP TIMER” on page 217

SET GVRP TIMER

Syntax

```
set gvrp timer join|leave|leaveall <1-65535> ge<1-28>
```

Parameters

default	Returns the GARP timers to their default settings.
join	Specifies the Join timer for joining the group. Enter a value in centiseconds, which are one hundredths of a second. The default is 20 centiseconds.
leave	Specifies the Leave timer for leaving a group. Enter a value in centiseconds, which are one hundredths of a second. The default is 60 centiseconds.
leaveall	Specifies the LeaveAll timer for leaving all groups. Enter a value in centiseconds, which are one hundredths of a second. The default is 1,000 centiseconds.
<1-65535>	Specifies the timer value in hundredths of a second. Enter a value between 1 and 65,535.
ge<1-28>	Specifies a port. There are 28 ports on the 9000/28 switch. To specify a port, precede the port number with "ge."

Description

Use the SET GVRP TIMER command to set the GARP timers to join or leave a group.

Note

You must make the settings for these timers the same on all GVRP-active network devices.

Examples

The following command sets the Join timer to 0.1 second for all GVRP applications on port 8:

```
switch#configure terminal
switch(config)#set gvrp timer join 10 ge8
```

The following commands set the leave timer to 0.5 seconds for all GVRP applications on port 9:

```
switch#configure terminal
```

```
switch(config)#set gvrp timer leave 50 seconds ge9
```

Related Commands

“SET GVRP” on page 212

“SET GVRP APPLICANT” on page 213

“SET GVRP DYNAMIC-VLAN-CREATION” on page 214

“SET GVRP REGISTRATION” on page 215

Chapter 8

Port Security Commands

The Port Security feature is based on assigning and limiting MAC addresses learned by a port. You can use the MAC-Address-based Port Security feature to enhance the security of your network by controlling which end nodes can forward frames through the switch, thereby preventing unauthorized individuals from accessing your network. This feature uses a MAC address to determine whether the switch should forward a frame or discard it. The source address is the MAC address of the end node that sent the frame.

All of the port security commands are available in the Interface Configuration mode.

This chapter contains the following commands:

- ❑ “SWITCHPORT PORT-SECURITY MAC-ADDRESS” on page 220
- ❑ “SWITCHPORT PORT-SECURITY MAXIMUM” on page 222
- ❑ “SWITCHPORT PORT-SECURITY MODE” on page 223
- ❑ “SWITCHPORT PORT-SECURITY VIOLATION” on page 225

Note

For port security configuration procedures, see “Setting Port Security” on page 46.

SWITCHPORT PORT-SECURITY MAC-ADDRESS

Syntax

```
switchport port-security mac-address sticky  
xxxx.xxxx.xxxx vlan <2-4094>
```

```
no switchport port-security mac-address sticky  
xxxx.xxxx.xxxx vlan <2-4094>
```

Parameters

mac-address Sets a predefined MAC dress in the following format:

xxxx.xxxx.xxxx

vlan Sets the VLAN ID. Choose a value between 2 and 4,094. You may not choose the default VLAN which has a VLAN ID of 1.

Description

Use the SWITCHPORT PORT-SECURITY MAC-ADDRESS command to set a predefined, secure MAC address for the specified port. This is an optional command that is used in conjunction with the SWITCHPORT PORT-SECURITY MAXIMUM command which sets the maximum number of MAC addresses that can be learned by a port.

If you configure fewer secure MAC addresses than the value specified in the SWITCHPORT PORT-SECURITY MAXIMUM command, then the remaining MAC addresses are learned dynamically.

In addition, you can specify which VLAN the MAC address can be learned on. If you do not specify a VLAN, then the MAC address can be learned on any VLAN.

Use the no form of this command to remove the predefined MAC address and VLAN ID.

Command Mode

Interface Configuration mode

Example

The following commands set the predefined MAC address of 00A0.0490.10E0 on port 7 and limits the VLAN to VLAN 7:

```
switch#configure terminal
```

```
switch(config)#interface ge7
```

```
switch(config-if)#switchport port-security mac-address  
00A0.0490.10E0 vlan 2
```

Related Commands

“SWITCHPORT PORT-SECURITY MAXIMUM” on page 222

“SWITCHPORT PORT-SECURITY MODE” on page 223

“SWITCHPORT TRUNK ALLOWED VLAN” on page 190

SWITCHPORT PORT-SECURITY MAXIMUM

Syntax

```
switchport port-security maximum <1-320>  
no switchport port-security maximum <1-320>
```

Parameters

maximum Sets the maximum number of MAC addresses that can be accepted by the port. Choose a value between 1 and 320.

Description

Use the SWITCHPORT PORT-SECURITY MAXIMUM command to set the maximum number of secure MAC addresses that can be learned by the specified port.

Use the no form of this command to remove maximum the port-security setting.

To display the current port security settings, use the “SHOW RUNNING-CONFIG INTERFACE” on page 160.

Command Mode

Interface Configuration mode

Example

The following commands set the maximum number of secure addresses learned on port 15 to 40:

```
switch#configure terminal  
switch(config)#interface ge15  
switch(config-if)#switchport port-security maximum 40
```

Related Commands

“SWITCHPORT PORT-SECURITY MODE” on page 223

“SWITCHPORT TRUNK ALLOWED VLAN” on page 190

SWITCHPORT PORT-SECURITY MODE

Syntax

```
switchport port-security mode limited|locked|secured

no switchport port-security mode
limited|locked|secured
```

Parameters

mode	Sets the security mode. Choose from the following options:	
limited		Sets the port to the Limited security mode. The port learns a limited number of dynamic MAC addresses. This is the least secure option.
locked		Sets the switch to the Locked security mode. The port stops learning new dynamic MAC addresses. The port forwards frames based on static MAC addresses and on those dynamic addresses it has already learned.
secured		Sets the port to the Secured security mode. The port accepts frames based only on static MAC addresses. You must enter the static MAC addresses of the nodes with frames the port is to accept after you have activated this security mode on a port. To add static MAC addresses, use the SWITCH-PORT PORT-SECURITY MAC-ADDRESS command.

Description

Use the SWITCHPORT PORT-SECURITY MODE command to set a port's security mode. Only one mode can be active on a port at a time. By default, no port-security mode is configured on an interface.

The no form of this command removes the current setting.

To display the current port security settings, use the "SHOW RUNNING-CONFIG INTERFACE" on page 160.

Command Mode

Interface Configuration mode

Example

The following commands set the security mode to “locked” on port 20:

```
switch#configure terminal
```

```
switch(config)#interface ge20
```

```
switch(config-if)#switchport port-security mode locked
```

Related Commands

“SWITCHPORT PORT-SECURITY MAC-ADDRESS” on page 220

“SWITCHPORT PORT-SECURITY MAXIMUM” on page 222

“SWITCHPORT TRUNK ALLOWED VLAN” on page 190

SWITCHPORT PORT-SECURITY VIOLATION

Syntax

```
switchport port-security violation  
protect|restrict|shutdown
```

```
no switchport port-security violation  
protect|restrict|shutdown
```

Parameters

violation Sets the security mode. Choose from the following options:

- | | |
|----------|--|
| protect | Permits traffic from a secure port only. Drops packets from insecure ports. This is the least secure option. |
| restrict | Sends an alert when security violation is detected. |
| shutdown | Shuts down port if a security violation is detected. |

Description

Use the SWITCHPORT PORT-SECURITY VIOLATION command to set a port's security mode. This is the action the software takes when the port has exceeded its maximum number of MAC addresses. Only one mode can be active on a port at a time. By default, no port-security mode is configured on an interface.

The no form of this command removes the current setting.

To display the current port security settings, use the "SHOW RUNNING-CONFIG INTERFACE" on page 160.

Command Mode

Interface Configuration mode

Example

The following commands set port 4 to shutdown when the AT-S100 software detects a security violation:

```
switch#configure terminal  
switch(config)#interface ge4  
switch(config-if)#switchport port-security violation  
shutdown
```

Related Commands

“SWITCHPORT PORT-SECURITY MAC-ADDRESS” on page 220

“SWITCHPORT PORT-SECURITY MAXIMUM” on page 222

“SWITCHPORT TRUNK ALLOWED VLAN” on page 190

Chapter 9

Simple Network Management Protocol (SNMP) Commands

This chapter provides descriptions of SNMP v1 and v2c commands that are accessed through the Configuration Terminal mode.

This chapter contains the following commands:

- ❑ “SNMP-SERVER COMMUNITY” on page 228
- ❑ “SNMP-SERVER CONTACT” on page 230
- ❑ “SNMP-SERVER ENABLE” on page 232
- ❑ “SNMP-SERVER GROUP” on page 233
- ❑ “SNMP-SERVER HOST” on page 235
- ❑ “SNMP-SERVER USER” on page 237
- ❑ “SNMP-SERVER USER REMOTE” on page 239
- ❑ “SNMP-SERVER VIEW” on page 241

SNMP-SERVER COMMUNITY

Syntax

```
snmp-server community STRING view VIEWNAME ro|rw|view
no snmp-server community
```

Parameters

STRING	Specifies the name of the SNMP community. Choose an alphanumeric value between 1 and 255 characters. This name acts as a password and permits access to SNMP.
VIEWNAME	Indicates the name of a view that was defined with the SNMP-SERVER VIEW command. Choose from the following options:
ro	Specifies the view is read-only access.
rw	Specifies the view is read-write access.
view	Specifies the MIB view.

Description

Use the SNMP-SERVER COMMUNITY command to set the name, view, and access of an SNMP community.

Use the no form of this command to remove a community string.

Command Mode

Configuration Terminal mode

Example

The following commands sets the name of the SNMP community to “engineering 78” and the view to read-write access:

```
switch#configure terminal
switch#(config)#snmp-server community “engineering 78”
rw
```

Related Commands

“SNMP-SERVER GROUP” on page 233

“SNMP-SERVER VIEW” on page 241

SNMP-SERVER CONTACT

Syntax

```
snmp-server contact LINE
```

```
no snmp-server contact
```

Parameters

LINE Specifies an alphanumeric string including spaces. You do not have to use quotation marks to indicate spaces. Choose a value that is between 1 and 255 characters in length.

Description

Use the SNMP-SERVER CONTACT command to set a contact person, email address, or IP address for the SNMP system. To remove a contact from the SNMP server, use the no form of this command.

Command Mode

Configuration Terminal mode

Examples

The following commands set the SNMP server contact to info@alliedtelesis.com:

```
switch#configure terminal
switch#(config)#snmp-server contact
info@alliedtelesis.com
```

The following commands set the SNMP server contact to "Todd Marcus:"

```
switch#configure terminal
switch#(config)#snmp-server contact Todd Marcus
```

The following commands set the SNMP server contact to IP address 192.34.12.4:

```
switch#configure terminal
switch#(config)#snmp-server contact 192.34.12.4
```

Related Commands

“SNMP-SERVER USER” on page 237

SNMP-SERVER ENABLE

Syntax

```
snmp-server enable  
no snmp-server enable
```

Parameters

none

Description

Use the SNMP-SERVER ENABLE command to enable SNMP link and failure traps on the switch. Use the no form of this command to disable SNMP link and failure traps.

Command Mode

Configuration Terminal mode

Example

The following commands enable an SNMP agent on the switch:

```
switch#configure terminal  
switch(config)#snmp-server enable
```

Related Commands

“SNMP-SERVER COMMUNITY” on page 228

SNMP-SERVER GROUP

Syntax

```
snmp-server group GROUPNAME v1|v2c auth|noauth|priv
|read[VIEWNAME]|write[VIEWNAME]|notify[VIEWNAME]
```

```
no snmp-server group GROUPNAME v1|v2c
```

Parameters

GROUPNAME	Specifies the group name. Choose an alphanumeric value between 1 and 255 characters.
v1	Specifies a group that uses the SNMPv1 security mode.
v2c	Specifies a group that uses the SNMPv2c security mode.
read	Specifies the view that permits the user read access. VIEWNAME Indicates a name of a view defined with the SNMP-SERVER VIEW command.
write	Specifies the view that the user is allowed to read and write. VIEWNAME Indicates a name of a view defined with the SNMP-SERVER VIEW command.
notify	Specifies the view that permits a user to be notified. VIEWNAME Indicates a name of a view defined with the SNMP-SERVER VIEW command.

Description

Use the SNMP-SERVER GROUP command to define the access rights for an SNMP group that you created with the SNMP-SERVER USER command. The SNMP-SERVER GROUP command assigns a security model and a security level to a group.

Use the no form of this command to remove an SNMP group.

Command Mode

Configuration Terminal mode

Examples

The following commands create an SNMPv1 group named “marcom” with write access to a view of the Internet which has an IP address of 1.3.6.1:

```
switch#configure terminal  
  
switch(config)#snmp-server group marcom v1 write  
1.3.6.1
```

The following commands create an SNMPv1 group named “group1” with access to a view called “nview” with notify permission:

```
switch#configure terminal  
  
switch(config)#snmp-server group group1 v1 notify  
nview
```

The following commands create an SNMPv2c group named “group2” with access to a view called “wview” with write permission and a view called “nview” with notify permission:

```
switch#configure terminal  
  
switch(config)#snmp-server group group2 v2c write  
wview notify nview
```

Related Commands

“SNMP-SERVER USER” on page 237

“SNMP-SERVER VIEW” on page 241

SNMP-SERVER HOST

Syntax

```
snmp-server host A.B.C.D informs|traps version 1|2c
COMMUNITY-STRING
```

```
no snmp-server host A.B.C.D informs|traps version 1|2c
COMMUNITY-STRING
```

Parameters

A.B.C.D	Specifies the name or the Internet address of the host.
inform	Sends SNMP inform messages to the host specified.
traps	Sends SNMP traps to the host specified.
version	Specifies the SNMP version used to send the traps. Choose from the following: <div> <div>1</div> <div>Indicates SNMPv1 traps.</div> </div> <div> <div>2c</div> <div>Indicates SNMPv2c traps.</div> </div>
COMMUNITY-STRING	Specifies the password community string that is sent with the notification operation. There is no default for this parameter.

Description

Use the SNMP-SERVER HOST command to create an SNMP v1 or v2c host which is the recipient of SNMP notifications. In addition, you define which SNMP mode (v1 or v2c) the host is able to receive.

Use the no form of the command to remove one or more of the following:

- ☐ the specified host
- ☐ specific traps that the host can receive
- ☐ the community-string.

Command Mode

Configuration Terminal mode

Examples

The following commands create an SNMP v2c host with an IP address of 192.34.10.1, traps, and public notification:

```
switch#configure terminal
```

```
switch(config)#snmp-server host 192.34.10.1 traps  
version 2c public
```

The following commands create an SNMP v1 host with an IP address of 192.34.10.1 that receives inform messages:

```
switch#configure terminal
```

```
switch(config)#snmp-server host 192.34.10.1 inform  
version 1
```

Related Commands

“SNMP-SERVER COMMUNITY” on page 228

“SNMP-SERVER USER” on page 237

SNMP-SERVER USER

Syntax

```
snmp-server user USERNAME GROUPNAME remote HOST
udpport <1-65536> v1|v2 auth(md5|sha) auth-password

no snmp-server user USERNAME
```

Parameters

USERNAME	Specifies the name of the user.
GROUPNAME	Specifies the name of the SNMP group. The user listed in this command becomes a member of this group.
HOST	Specifies the IP address of the host that connects to the agent in the following format: xxx.xxx.xxx.xxx
udp-port	Specifies a UDP port value. Enter a value between 1 and 65536. The default value is 162.
v1	Specifies the SNMPv1 security mode.
v2c	Specifies the SNMPv2c security mode.
auth	Specifies authentication is used to verify the server. If you select this parameter, you must specify an auth-password. md5 Specifies the MD5 security mode. This is an optional parameter. sha Specifies the SHA security mode. This is an optional parameter.
auth-password	Specifies the SNMP authorization password.

Description

Use the SNMP-SERVER USER command to create an SNMP user, create an SNMP group, and assign the user to an SNMP group. In addition, the SNMP-SERVER USER command maps a security mode, authentication mode, and authorization password to a group name.

Use the no form of the SNMP-SERVER USER command to remove an SNMP user from a group.

Command Mode

Configuration Terminal mode

Examples

The following commands add a user named Marla to the group called ati3 which is an SNMPv2c group connected to a host with an IP address of 192.168.9.1. In addition, the UDP port assigned is 170, the security mode is MD5, and the authorization password is “funnybusiness14:”

```
switch#configure terminal
```

```
switch(config)#snmp-server user Marla ati3 remote  
192.168.9.1 v2 udp-port 170 auth md5 funnybusiness14
```

The following commands remove a user named Xifan:

```
switch#configure terminal
```

```
switch(config)#no snmp-server user xifan
```

Related Commands

“SNMP-SERVER GROUP” on page 233

SNMP-SERVER USER REMOTE

Syntax

```
snmp-server user remote GROUPNAME remote A.B.C.D udp-  
port PORT<1-65535> encrypted auth(md5|sha) password  
PASSWORD
```

```
no snmp-server user USERNAME
```

Parameters

USERNAME	Specifies the name of the user.
GROUPNAME	Specifies the name of the SNMP group. The user listed in this command becomes a member of this group.
A.B.C.D	Specifies the IP address of the host that connects to the agent in the following format: xxx.xxx.xxx.xxx
PORT	Specifies the UDP port. Choose a value between 1 and 65,535. The default value is 162.
encrypted	Enables an encrypted password. This is an optional parameter.
auth	Specifies authentication is used to verify the server. If you select this parameter, you must specify the SNMP authorization password. md5 Specifies the MD5 security mode. This is an optional parameter. sha Specifies the SHA security mode. This is an optional parameter.
PASSWORD	Specifies the SNMP authorization password.

Description

Use the SNMP-SERVER USER command to create an SNMP user, create an SNMP group, and assign the user to an SNMP group. In addition, the SNMP-SERVER USER command maps a security mode and security name to a group name.

Use the no form of this command to remove an SNMP user from a group.

Command Mode

Configuration Terminal mode

Example

The following commands add a user named Shufen to an SNMPv2c group called ati3 which is connected to a host with an IP address of 192.168.10.1. A password defined as “super1password” is used as an authorization password:

```
switch#configure terminal
```

```
switch(config)#snmp-server user shufen remote ati3  
192.168.10.1 v2 auth SHA super1password
```

Related Commands

“SNMP-SERVER GROUP” on page 233

“SNMP-SERVER USER” on page 237

SNMP-SERVER VIEW

Syntax

```
snmp-server view VIEWNAME WORD include|exclude  
no snmp-server view
```

Parameters

VIEWNAME	Specifies the name of the user.
WORD	Specifies the MIB Tree.
include	Includes users in this view.
exclude	Excludes users from this view.

Description

Use the SNMP-SERVER VIEW command to create an SNMP view and determine if a user can access it. The MIB tree is defined by RFC 1155 Structure of Management Information. You use object identifiers (OIDs) to specify MIB modules that are included or excluded in a view. After you create a view, you can map an SNMP group to it with the SNMP-SERVER GROUP command.

Use the no form of this command to remove an SNMP view.

Command Mode

Configuration Terminal mode

Examples

The following commands create a view called "Internet" and allows the users that are mapped to this Object Identifier (OID) to view the Internet:

```
switch#configure terminal  
switch(config)#snmp-server view Internet 1.3.6.1  
include
```

The following commands create a view called "sweng4" and excludes users that are mapped to this OID from viewing its contents:

```
switch#configure terminal  
switch(config)#snmp-server view sweng4 1.3.6.1.4.1  
exclude
```

Related Commands

“SNMP-SERVER GROUP” on page 233

Chapter 10

Spanning Tree Protocol (STP) Commands

The commands in this chapter can be used in the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) Protocol daemons. All of the spanning-tree commands are available in the Configuration Terminal mode.

This chapter contains the following commands:

- ❑ “SHOW SPANNING-TREE” on page 244
- ❑ “SPANNING-TREE ENABLE FORWARD” on page 247
- ❑ “SPANNING-TREE FORWARD-TIME” on page 249
- ❑ “SPANNING-TREE HELLO-TIME” on page 250
- ❑ “SPANNING-TREE MAX-AGE” on page 251
- ❑ “SPANNING-TREE MODE” on page 252
- ❑ “SPANNING-TREE PORTFAST BPDU-FILTER DEFAULT” on page 253
- ❑ “SPANNING-TREE PORTFAST BPDU-GUARD DEFAULT” on page 254
- ❑ “SPANNING-TREE PRIORITY” on page 255

Note

To display the current spanning tree configuration, see “SHOW SPANNING-TREE” on page 106.

SHOW SPANNING-TREE

Syntax

```
show spanning-tree interface INTERFACE ge<1-28>
```

Parameters

INTERFACE Indicates the name of an interface. Specify ports ge1 through ge28

Description

Use the SHOW SPANNING-TREE command to display the status of the active spanning tree protocol on the specified port.

Command Mode

Privileged Executive mode

Example

The following command displays the spanning tree configuration on port 1:

```
switch#show spanning-tree interface ge1
```

This command displays a variety of parameters. An example of page 1 of the display is shown in Figure 27.

```
(switch3)# show spanning-tree interface ge1
% 1: Bridge up - Spanning Tree Disabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000012341212ab
% 1: Bridge Id 80000012341212ab
% 1: last topology change Sat Jan 1 00:00:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% 1:   ge1: Port 2001 - Id 87d1 - Role Disabled - State Fwd
% 1:   ge1: Designated Path Cost 0
% 1:   ge1: Configured Path Cost 200000 - Add type Explicit ref
count 1
% 1:   ge1: Designated Port Id 87d1 - Priority 128 -
% 1:   ge1: Root 80000012341212ab
% 1:   ge1: Designated Bridge 80000012341212ab
% 1:   ge1: Message Age 0 - Max Age 20
% 1:   ge1: Hello Time 2 - Forward Delay 15
% 1:   ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 -
topo change timer 0
% 1:   ge1: forward-transitions 2
% 1:   ge1: Version Rapid Spanning Tree Protocol - Received None
Send RSTP
--More--
```

Figure 27. SHOW SPANNING-TREE Command, page 1

See Figure 28 for page 2 of the display.

```
% 1:   ge1: No portfast configured - Current portfast off
% 1:   ge1: portfast bpdu-guard default - Current portfast bpdu-
guard off
% 1:   ge1: portfast bpdu-filter default - Current portfast bpdu-
guard off
% 1:   ge1: no root guard configured - Current root guard off
% 1:   ge1: Configured Link Type point-to-point - Current point-
to-point
%
(switch3)#
```

Figure 28. SHOW SPANNING-TREE Command, page 2

Related Commands

“SPANNING-TREE MODE” on page 252

SPANNING-TREE ENABLE FORWARD

Syntax

```
spanning-tree stp|rstp enable forward
```

```
no spanning-tree stp|rstp enable forward
```

Parameters

stp	Specifies IEEE 801.Q Spanning-tree protocol (STP).
rstp	Specifies IEEE 801.w rapid Rapid Spanning-tree protocol (RSTP).
enable	Makes the current spanning tree protocol the active spanning-tree protocol.
forward	Allows the ports on the switch to transmit and receive traffic regardless if a spanning tree protocol is enabled on the switch.

Description

Use the SPANNING-TREE ENABLE command to enable STP or RSTP on the switch. After you have specified a spanning tree protocol, such as RSTP, all subsequent spanning tree commands in a login session apply to this spanning tree protocol. To make the specified spanning tree protocol the active spanning tree mode and enable it on the switch, use the SPANNING TREE MODE command.

Use the no form of this command to disable the spanning tree protocol on the switch.



Caution

Allied Telesis recommends using the NO SPANNING-TREE STP|RSTP ENABLE FORWARD command to disable a spanning tree protocol. If this command is used without the "FORWARD" parameter, it disables the spanning-tree protocol and prevents all of the ports from receiving or transmitting data. This causes loss of data.

Command Mode

Configuration Terminal mode

Examples

The following commands enable RSTP on the switch:

```
switch#configure terminal
```

```
switch(config)#spanning-tree rstp enable forward
```

The following commands disable STP on the switch while still allowing the ports to transmit and receive traffic:

```
switch#configure terminal
```

```
switch(config)#no spanning-tree stp enable forward
```

Related Commands

“SPANNING-TREE MODE” on page 252

SPANNING-TREE FORWARD-TIME

Syntax

```
spanning-tree forward-time <4-30>  
no spanning-tree forward-time
```

Parameters

none

Description

Use the SPANNING-TREE FORWARD-TIME command to set the time, (in seconds), after which (if this bridge is the root bridge) each interface changes to the learning and forwarding states. This value is used by all instances. The default value is 15 seconds.

Use the no form of this command to restore the default value of 15 seconds.

Command Mode

Configuration Terminal mode

Example

The following commands set the forward delay time to 20 seconds:

```
switch#configure terminal  
switch(config)#spanning-tree forward-time 20
```

Related Commands

“SPANNING-TREE MAX-AGE” on page 251

SPANNING-TREE HELLO-TIME

Syntax

```
spanning-tree hello-time <1-10>
```

```
no spanning-tree hello-time
```

Parameters

none

Description

Use the SPANNING-TREE HELLO-TIME command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). A very low value of this command leads to excessive traffic on the network, while a higher value delays the detection of topology change. This value is used by all instances.

To restore the default value of the hello time, use the no form of this command.

Command Mode

Configuration Terminal mode

Example

The following commands set the hello delay time to 9 seconds:

```
switch#configure terminal
```

```
switch(config)#spanning-tree hello-time 9
```

Related Commands

none

SPANNING-TREE MAX-AGE

Syntax

```
spanning-tree max-age <6-40>
```

```
no spanning-tree max-age
```

Parameters

none

Description

Use the SPANNING-TREE MAX-AGE command to set the max-age for a bridge. Max-age is the maximum time, in seconds, for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. This value is used by all instances.

Set the value of max-age to greater than twice the value of the hello time plus one, but less than twice the value of forward delay minus one. The allowable range for max-age is 6-40 seconds. The default value is 20 seconds.

Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the max-age.

Use the no form of this command to restore the default value of max-age.

Command Mode

Configuration Terminal mode

Example

The following commands set the max-age time for the bridge to 10 seconds:

```
switch#configure terminal
```

```
switch(config)#spanning-tree max-age 10
```

Related Commands

“SPANNING-TREE FORWARD-TIME” on page 249

SPANNING-TREE MODE

Syntax

```
spanning-tree mode stp|rstp  
no spanning-tree mode
```

Parameters

stp Specifies IEEE 801.Q Spanning-tree protocol (STP).
rstp Specifies IEEE 801.w rapid Rapid Spanning-tree protocol (RSTP).

Description

Use the SPANNING-TREE MODE command to specify the active Spanning Tree Protocol and enable it on the switch. The default value is RSTP.

Use the no form of this command to restore RSTP as the default value.

Command Mode

Configuration Terminal mode

Example

The following commands set the active spanning tree mode to STP and enables this mode on the switch:

```
switch#configure terminal  
switch(config)#spanning-tree mode stp
```

Related Commands

“SPANNING-TREE ENABLE FORWARD” on page 247

SPANNING-TREE PORTFAST BPDU-FILTER DEFAULT

Syntax

```
spanning-tree portfast bpdu-filter default
no spanning-tree portfast bpdu-filter default
```

Parameters

none

Description

Use the SPANNING-TREE BPDU-FILTER DEFAULT command to globally enable the BPDU filter on a bridge.

The Spanning Tree Protocol sends BPDUs from all interfaces. Enabling the BPDU filter ensures that portfast-enabled interfaces do not transmit or receive any BPDUs.

Use the no form of this command to disable the BPDU filter on a bridge.

Command Mode

Configuration Terminal mode

Example

The following commands enable the BPDU filter on a bridge:

```
switch#configure terminal
switch(config)#spanning-tree portfast bpdu-filter
default
```

Related Commands

“SPANNING-TREE PORTFAST BPDU-GUARD DEFAULT” on page 254

SPANNING-TREE PORTFAST BPDU-GUARD DEFAULT

Syntax

```
spanning-tree portfast bpdu-guard default  
no spanning-tree portfast bpdu-guard default
```

Parameters

none

Description

Use the SPANNING-TREE BPDU-GUARD DEFAULT command to enable the BPDU (Bridge Protocol Data Unit) guard feature on a bridge. This command indicates the bridge level BPDU-Guard configuration takes effect.

When the BPDU guard feature is set for a bridge, all portfast-enabled interfaces of the bridge that have the BPDU guard set to default shut down the interface on receiving a BPDU. In this case, the BPDU is not processed. You can bring the interface up manually by using the NO SHUTDOWN command.

Use the no form of the SPANNING-TREE BPDU-GUARD command to disable the BPDU-guard feature on a bridge.

Command Mode

Configuration Terminal mode

Example

The following commands enable the BPDU Guard feature on a bridge:

```
switch#configure terminal  
switch(config)#spanning-tree portfast bpdu-guard
```

Related Commands

“SHUTDOWN” on page 181

“SPANNING-TREE PORTFAST BPDU-FILTER DEFAULT” on page 253

SPANNING-TREE PRIORITY

Syntax

`spanning-tree priority <0-61440>`

`no spanning-tree priority`

Parameters

`<0-61440>` Specifies the bridge priority value in increments of 4,096. For example, 4,096, 8,192, and 12,288 are all valid values.

Description

Use the SPANNING-TREE PRIORITY command to specify the interface priority. A lower priority value indicates a greater likelihood of becoming a root. The default value is 32,768.

The no form of this command resets the spanning-tree priority value to the default value which is 32,768.

Note

This command can be used for either STP or RSTP.

Command Mode

Configuration Terminal mode

Example

The following commands set the spanning-tree priority on the switch to 4,096:

```
switch#configure terminal
```

```
switch(config)#spanning-tree priority 4096
```

Related Commands

none

Chapter 11

Virtual Local Area Networks (VLAN) Commands

This chapter provides descriptions of VLAN commands that are accessed through the Configuration Terminal mode.

This chapter contains the following commands:

- ❑ “SHOW VLAN ALL” on page 258
- ❑ “SHOW VLAN BRIEF” on page 260
- ❑ “SHOW VLAN DYNAMIC” on page 262
- ❑ “SHOW VLAN STATIC” on page 263
- ❑ “SWITCHPORT TRUNK ALLOWED VLAN” on page 265
- ❑ “VLAN” on page 267
- ❑ “VLAN ACCESS-MAP” on page 268
- ❑ “VLAN DATABASE” on page 269

SHOW VLAN ALL

Syntax

```
show vlan all
```

Parameters

none

Description

Use the SHOW VLAN ALL command to display information about all of the VLANs, both static and dynamic, configured on the switch.

Command Mode

Privileged Executive mode

Example

The following example shows the SHOW VLAN ALL command and a sample of the output:

```
switch3#show vlan all
```

See Figure 29 for an example display.

```
(switch3)# show vlan all
VLAN ID      Name          Type      State      Member ports
=====      =====      =====      =====      =====
1            default      STATIC    ACTIVE      ge1(u) ge2(u) ge3(u) ge4(u) ge6(u)
              ge8(u) ge9(u) ge10(u) ge11(u) ge12(u)
              ge13(u) ge14(u) ge15(u) ge16(u)
              ge17(u) ge18(u) ge19(u) ge20(u)
              ge21(u) ge22(u) ge23(u) ge24(u)
              ge25(u) ge26(u) ge27(u) ge28(u) ge7(u)
3            VLAN0003     STATIC    ACTIVE      ge5(u) ge7(t)
4            VLAN0004     STATIC    ACTIVE      ge7(t)
```

Figure 29. SHOW VLAN ALL

Related Commands

“SHOW MAC ADDRESS-TABLE VLAN” on page 102

“SHOW VLAN BRIEF” on page 260

“SHOW VLAN DYNAMIC” on page 262

“SHOW VLAN STATIC” on page 263

SHOW VLAN BRIEF

Syntax

```
show vlan brief
```

Parameters

none

Description

Use the SHOW VLAN BRIEF command to display information about all of the VLANs, both static and dynamic, configured on the switch.

Command Mode

Privileged Executive mode

Example

The following example shows the SHOW VLAN BRIEF command and a sample of the output:

```
switch3#show vlan brief
```

See Figure 30 for an example display.

```
(switch3)# show vlan brief
VLAN ID    Name        Type        State        Member ports
=====    =====    =====    =====    =====
1          default     STATIC      ACTIVE      ge1(u) ge2(u) ge3(u) ge4(u) ge6(u)
                                     ge8(u) ge9(u) ge10(u) ge11(u) ge12(u)
                                     ge13(u) ge14(u) ge15(u) ge16(u)
                                     ge17(u) ge18(u) ge19(u) ge20(u)
                                     ge21(u) ge22(u) ge23(u) ge24(u)
                                     ge25(u) ge26(u) ge27(u) ge28(u) ge7(u)
3          VLAN0003    STATIC      ACTIVE      ge5(u) ge7(t)
4          VLAN0004    STATIC      ACTIVE      ge7(t)
```

Figure 30. SHOW VLAN BRIEF

Related Commands

“SHOW MAC ADDRESS-TABLE VLAN” on page 102

“SHOW VLAN ALL” on page 258

“SHOW VLAN BRIEF” on page 260

“SHOW VLAN DYNAMIC” on page 262

“SHOW VLAN STATIC” on page 263

SHOW VLAN DYNAMIC

Syntax

```
show vlan dynamic
```

Parameters

none

Description

Use the SHOW VLAN DYNAMIC command to display information about dynamic VLANs on the switch.

Command Mode

Privileged Executive mode

Example

The following example shows the SHOW VLAN DYNAMIC command and a sample of the output:

```
switch3#show vlan dynamic
```

See Figure 31 for an sample display.

```
(switch3)# show vlan dynamic
VLAN ID      Name          Type      State      Member ports
=====      =====      =====      =====      =====
          (u)-Untagged, (t) Tagged
9            VLAN0009      DYNAMIC    ACTIVE      ge11(u) ge12(u) ge33(u) ge14(u)
```

Figure 31. SHOW VLAN DYNAMIC

Related Commands

“SHOW VLAN ALL” on page 258

“SHOW VLAN BRIEF” on page 260

“SHOW VLAN STATIC” on page 263

SHOW VLAN STATIC

Syntax

show vlan static

Parameters

none

Description

Use the SHOW VLAN STATIC command to display information about all of the VLANs, both static and dynamic, configured on the switch.

Command Mode

Privileged Executive mode

Example

The following example shows the SHOW VLAN STATIC command and a sample of the output:

switch3#show vlan static

See Figure 32 for an sample display.

(switch3)# show vlan static

VLAN ID	Name	Type	State	Member ports (u)-Untagged, (t) Tagged
=====	=====	=====	=====	=====
1	default	STATIC	ACTIVE	ge1(u) ge2(u) ge3(u) ge4(u) ge6(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u) ge25(u) ge26(u) ge27(u) ge28(u) ge7(u)
3	VLAN0003	STATIC	ACTIVE	ge5(u) ge7(t)
4	VLAN0004	STATIC	ACTIVE	ge7(t)

Figure 32. SHOW VLAN STATIC

Related Commands

“SHOW VLAN ALL” on page 258

“SHOW VLAN BRIEF” on page 260

“SHOW VLAN DYNAMIC” on page 262

SWITCHPORT TRUNK ALLOWED VLAN

Syntax

```
switchport trunk allowed vlan add|remove VLANID
no switchport trunk vlan
```

Parameters

- | | |
|--------|---|
| add | Add a VLAN to transmit and receive through the Layer-2 interface. |
| remove | Remove a VLAN that transmits and receives through the Layer-2 interface. |
| VLANID | Specifies a VLAN ID or a list of VLAN IDs. Enter a value from 2 to 4094. Set a single VLAN, VLAN range, or a VLAN list.

For a VLAN range, specify the lowest VLAN, then the highest VLAN number in the range, and separate them with a hyphen.

For a VLAN list, specify VLAN IDs separated by commas. |

Note

Do not enter spaces between hyphens or commas when setting parameters for VLAN ranges or lists.

Description

Use the SWITCHPORT TRUNK ALLOWED VLAN command to change the default VLAN for an interface. Use the no form of this command to remove a previously created VLAN with the specified VLAN ID.

Command Mode

Interface Configuration mode

Examples

The following commands add a single VLAN, VLAN 2, to the member set of port 6:

```
switch#configure terminal
switch(config)#interface ge6
```

```
switch(config-if)#switchport mode trunk
```

```
switch(config-if)#switchport trunk allowed vlan add 2
```

The following commands add VLANs 3 through 6 to the member set of port 7:

```
switch#configure terminal
```

```
switch(config)#interface ge7
```

```
switch(config-if)#switchport mode trunk
```

```
switch(config-if)#switchport trunk allowed vlan add 3-6
```

The following commands remove a list of VLANs from port 5:

```
switch#configure terminal
```

```
switch(config)#interface ge5
```

```
switch(config-if)#switchport mode trunk
```

```
switch(config-if)#switchport trunk allowed vlan remove
```

Related Commands

“SHOW VLAN ALL” on page 258

“SWITCHPORT MODE TRUNK” on page 188

VLAN

Syntax

```
vlan <2-4094> name NAME state enable|disable
```

Parameters

<2-4094>	Indicates the VLAN ID. Enter a value between 2 and 4094.				
name	Indicates the name of the VLAN. Enter a text value.				
state	Indicates the active state of the VLAN. Choose from the following: <table> <tr> <td>enable</td><td>Activates the VLAN.</td></tr> <tr> <td>disable</td><td>Inactivates the VLAN.</td></tr> </table>	enable	Activates the VLAN.	disable	Inactivates the VLAN.
enable	Activates the VLAN.				
disable	Inactivates the VLAN.				



Caution

You may not create a VLAN with a VLAN ID of 1. This is the default VLAN.

Command Mode

VLAN Configuration mode

Description

Use the VLAN command to create a VLAN, assign a name to it, and set the state of the VLAN.

Example

The following commands create a VLAN 2 with a name of “Sales” and enable it:

```
switch# configure terminal
switch(config)# vlan database
switch(config-vlan)# vlan 2 name sales state enable
```

Related Commands

“VLAN ACCESS-MAP” on page 268

“VLAN DATABASE” on page 269

VLAN ACCESS-MAP

Syntax

```
vlan access-map NAME <1-65535>
```

Parameters

NAME Specifies the name of the access map and the sequence to insert or delete it from an existing access-map entry.

Command Mode

Configuration Terminal mode

Description

Use the VLAN ACCESS-MAP command to create a VLAN access-map, name it, and determine the sequence to insert it to or delete it from an existing access map entry.

Example

The following commands create a VLAN access-map named “Map 4” and gives it a priority of 1:

```
switch# configure terminal  
switch(config)# vlan access-map “Map 4” 1
```

Related Commands

“VLAN” on page 267

VLAN DATABASE

Syntax

`vlan database`

Parameters

none

Command Mode

Configuration Terminal mode

Description

Use the VLAN DATABASE command to enter the VLAN configuration mode. After you enter the VLAN mode, the prompt changes to indicate the new mode and you can enter commands to add, delete, or modify values associated with a single VLAN.

Example

The following commands permits access to the VLAN Configuration mode and displays the new prompt that indicates the new mode:

```
switch# configure terminal
```

```
switch(config)# vlan database
```

```
switch(config-vlan)#
```

Related Commands

“VLAN” on page 267

Index

Numerics

802.1x Port-based Network Access Control
described 56
displaying status 57
DOT1X PORT-CONTROL command 165, 166, 198
enabling 56, 123, 199
LOGIN REMOTELOCAL command 200
RADIUS-SERVER HOST command 201
RADIUS-SERVER KEY command 202
setting 57
SHOW DOT1X ALL command 204
SHOW DOT1X command 203
SHOW DOT1X INTERFACE command 207
SHOW DOT1X STATISTICS INTERFACE command 209

C

CLEAR MAC ADDRESS-TABLE DYNAMIC command 33, 73
CLEAR MAC ADDRESS-TABLE MULTICAST command 75
CLEAR MAC ADDRESS-TABLE STATIC command 77
CLOCK SUMMER-TIME command 117
CLOCK TIMEZONE command 119
commands, formatting 24
community names
SNMPv1 and SNMPv2c 60
CONFIGURATION TERMINAL command 79
Configuration Terminal mode
assigning a password 124, 125
CLOCK SUMMER-TIME command 117
CLOCK TIMEZONE command 119
CRYPTO KEY GENERATE USERKEY command 121
DOT1X SYSTEM-AUTH-CTRL command 123, 199
ENABLE PASSWORD command 124
ENABLE SECRET command 125
EXIT command 88, 126, 167
exiting 88, 126, 167
HELP command 127
HOSTNAME command 128
INTERFACE command 129
IP IGMP SNOOPING command 131
IP ROUTE command 29, 132
IP SSH RSA KEYPAIR-NAME command 133, 134, 174
LINE CONSOLE command 135
LINE VTY command 136
MAC ADDRESS-TABLE AGEING-TIME command 33, 138

MAC ADDRESS-TABLE STATIC DISCARD command 34, 139
MAC ADDRESS-TABLE STATIC FORWARD command 34, 141
MLS QOS command 143
NTP AUTHENTICATE command 30, 145, 146
NTP SERVER command 29, 148
NTP TRUSTED-KEY command 30, 150
SHOW LIST command 151
SHOW RUNNING-CONFIG command 153
SHOW RUNNING-CONFIG FULL command 158
SPANNING-TREE ENABLE command 247
SPANNING-TREE FORWARD-TIME command 249
SPANNING-TREE HELLO-TIME command 250
SPANNING-TREE MAX-AGE command 251
SPANNING-TREE MODE command 252
SPANNING-TREE PORTFAST BPDU-FILTER command 253
SPANNING-TREE PORTFAST BPDU-GUARD command 254
SPANNING-TREE PRIORITY command 255
USERNAME command 31, 162
COPY DEFAULT.CFG command 82, 84
COPY RUNNING-CONFIG STARTUP-CONFIG command 31, 39, 81
CoS. *See* Class of Service (CoS)
CP command 86
CRYPTO KEY GENERATE USERKEY command 121

D

destination port in a port mirror 43
DHCP
IP ADDRESS DHCP command 29, 173
setting 29
document conventions 12
DOT1X PORT-CONTROL command 165, 166, 198
DOT1X SYSTEM-AUTH-CTRL command 123, 199
downgrading software 35
DOWNLOAD A.B.C.D FILE-NAME command 35
DOWNLOAD TFTP command 87

E

ENABLE PASSWORD command 124
ENABLE SECRET command 125
EXIT command 88, 126, 167

F

FLOW CONTROL BACKPRESSURE command 50, 168

FLOW CONTROL RECEIVE command 169
 FLOW CONTROL SEND command 50, 170

G

GARP

timer, setting 217

gateway address

setting 29

GVRP

creating dynamic VLANs 214
 disabling 53, 212
 disabling ports 213
 enabling 53, 212
 enabling dynamic VLANs 54
 enabling ports 213
 setting GVRP registration 54
 setting registration 215
 setting the applicant state 54
 setting the join and leave timers 55

H

help

selecting context-sensitive help 24

HELP command 127

HOSTNAME command 128

I

IGMP

enabling 55

interface

assigning secure MAC addresses 48
 creating port trunks 49, 184
 disabling backpressure 50
 disabling ports 45
 displaying 43, 90
 enabling backpressure 50
 enabling flow control 50
 enabling ports 45
 preventing broadcast storms 51
 setting duplex mode 44
 setting maximum number of MAC addresses 47
 setting MDI 45, 175
 setting MDIX 45, 175
 setting MTU value 31, 178
 setting port mirroring 43
 setting port security 46, 219
 setting port speed 44
 setting port-security violation 49, 225
 setting the maximum number of MAC addresses 220, 222
 setting the security mode 48, 223
 setting the threshold level 51, 185

INTERFACE command 129

Interface Configuration mode

FLOW CONTROL BACKPRESSURE command 50, 168
 FLOW CONTROL RECEIVE command 169
 FLOW CONTROL SEND command 50, 170
 IP ADDRESS command 28, 171

IP ADDRESS DHCP command 29, 173

SHOW RUNNING-CONFIG INTERFACE command 179

SHUTDOWN command 45, 181

SPEED command 44, 182

STATIC-CHANNEL-GROUP command 49, 184

Interface mode

accessing the Interface mode 129

HELP command 127

MDIX command 45, 175

MIRROR INTERFACE DIRECTION command mode 43, 176

MTU command 31, 178

SHOW RUNNING-CONFIG command 38, 153

SHOW RUNNING-CONFIG COMMUNITY-LIST command 158

SHOW RUNNING-CONFIG FULL command 104, 160

STORM-CONTROL command 51, 185

SWITCHPORT ACCESS VLAN command 41, 187

SWITCHPORT MODE TRUNK command 188

SWITCHPORT PORT-SECURITY MAXIMUM command 47, 48, 220, 222

SWITCHPORT PORT-SECURITY MODE command 48, 49, 223, 225

SWITCHPORT TRUNK ALLOWED VLAN command 42, 190, 265

TRAFFIC-CLASS-TABLE USER-PRIORITY NUM-TRAFFIC-CLASSES command 192

USER-PRIORITY command 193

IP address

assigning 28

IP ADDRESS command 28, 171

IP ADDRESS DHCP command 29, 173

IP IGMP SNOOPING command 131

IP ROUTE command 29, 132

IP SSH RSA KEYPAIR-NAME command 133, 134, 174

K

keyword abbreviations 24

L

LACP

setting 56

limited port security mode 46

LINE CONSOLE command 135

LINE VTY command 136

locked port security mode 47

log output

modifying 117, 119, 121

LOG TRAP command 117, 119, 121

LOGIN REMOTELOCAL command 200

LOGOUT command 89

M

MAC address

adding a static MAC address 34

assigning secure MAC addresses 48

clearing 33

displaying the MAC address table 32, 92

- removing a static MAC address 34
- setting 32
- setting a maximum number 47
- setting the aging time 33
- MAC address table
 - ageing time 138, 139
- MAC ADDRESS-TABLE AGEING-TIME command 33, 138
- MAC ADDRESS-TABLE STATIC DISCARD command 34, 139
- MAC ADDRESS-TABLE STATIC FORWARD command 34, 141
- MDI mode 45, 175
- MDIX command 45, 175
- MDIX mode 45, 175
- MIRROR INTERFACE DIRECTION command 43, 176
- MLS QOS command 143
- MTU command 31, 178

N

- Network Time Protocol (NTP)
 - specifying key numbers 30, 150
 - specifying the server IP address 29, 148
- Network Transport Protocol (NTP)
 - turning on authentication 30, 145, 146
- NTP AUTHENTICATE command 30, 145, 146
- NTP SERVER command 29, 148
- NTP TRUSTED-KEY command 30, 150

P

- port-based access control. See 802.1x Port-based Network Access Control
- Privileged Executive mode
 - CLEAR MAC ADDRESS-TABLE DYNAMIC command 33, 73
 - CLEAR MAC ADDRESS-TABLE MULTICAST command 75
 - CLEAR MAC ADDRESS-TABLE STATIC command 77
 - CONFIGURATION TERMINAL command 79
 - COPY DEFAULT.CFG command 82, 84
 - COPY RUNNING-CONFIG STARTUP-CONFIG command 31, 39, 81
 - CP command 86
 - DOWNLOAD A.B.C.D FILE-NAME command 35
 - DOWNLOAD TFTP command 87
 - HELP command 127
 - LOGOUT command 89
 - SHOW INTERFACE command 43, 90
 - SHOW MAC ADDRESS-TABLE AGING-TIME command 33, 94
 - SHOW MAC ADDRESS-TABLE command 32, 92
 - SHOW MAC ADDRESS-TABLE DYNAMIC command 96
 - SHOW MAC ADDRESS-TABLE INTERFACE command 98
 - SHOW MAC ADDRESS-TABLE STATIC command 100
 - SHOW MAC ADDRESS-TABLE VLAN command 102
 - SHOW RUNNING-CONFIG command 153
 - SHOW RUNNING-CONFIG FULL command 158

- SHOW RUNNING-CONFIG INTERFACE command 179
- SHOW SPANNING-TREE command 106, 244
- SHOW STATIC-CHANNEL-GROUP command 109
- SHOW USER-PRIORITY command 110
- SHOW VLAN ALL command 258
- SHOW VLAN BRIEF command 260
- SHOW VLAN DYNAMIC command 262
- SHOW VLAN STATIC command 263
- SYSTEM FACTORY-RESET command 35, 111
- SYSTEM REBOOT command 35, 112
- UPLOAD command 113

R

- RADIUS authentication
 - configuring 58
 - setting 59
- RADIUS-SERVER HOST command 201
- RADIUS-SERVER KEY command 202
- Rapid Spanning Tree Protocol (RSTP)
 - disabling 64
 - displaying 63
 - enabling 64
 - setting 62
 - setting priority 64

S

- Secure Shell (SSH)
 - described 62
 - setting 62
- secured port security mode 47
- SET GVRP APPLICANT command 213
- SET GVRP command 212
- SET GVRP DYNAMIC-VLAN-CREATION command 214
- SET GVRP REGISTRATION command 215
- SET GVRP TIMER command 217
- SHOW DOT1X ALL command 204
- SHOW DOT1X command 203
- SHOW DOT1X INTERFACE command 207
- SHOW DOT1X STATISTICS INTERFACE command 209
- SHOW INTERFACE command 43, 90
- SHOW LIST command 151
- SHOW MAC ADDRESS-TABLE AGING-TIME command 33, 94
- SHOW MAC ADDRESS-TABLE command 32, 92
- SHOW MAC ADDRESS-TABLE DYNAMIC command 96
- SHOW MAC ADDRESS-TABLE INTERFACE command 98
- SHOW MAC ADDRESS-TABLE STATIC command 100
- SHOW MAC ADDRESS-TABLE VLAN command 102
- SHOW RUNNING-CONFIG command 38, 153
- SHOW RUNNING-CONFIG COMMUNITY-LIST command 158
- SHOW RUNNING-CONFIG FULL command 104, 160
- SHOW RUNNING-CONFIG INTERFACE command 179
- SHOW SPANNING-TREE command 106, 244
- SHOW STATIC-CHANNEL-GROUP command 109
- SHOW USER-PRIORITY command 110
- SHOW VLAN ALL command 258
- SHOW VLAN BRIEF command 260

- SHOW VLAN DYNAMIC command 262
 - SHOW VLAN STATIC command 263
 - SHUTDOWN command 45, 181
 - SNMP
 - adding traps 61
 - creating communities 60
 - SNMP-SERVER COMMUNITY command 228
 - SNMP-SERVER CONTACT command 230
 - SNMP-SERVER ENABLE command 232
 - SNMP-SERVER GROUP command 233
 - SNMP-SERVER HOST command 235
 - SNMP-SERVER USER command 237, 239, 241
 - SNMP community strings
 - access mode 60
 - default 60
 - name 60
 - trap receivers 61
 - SNMP-SERVER COMMUNITY command 228
 - SNMP-SERVER CONTACT command 230
 - SNMP-SERVER ENABLE command 232
 - SNMP-SERVER GROUP command 233
 - SNMP-SERVER HOST command 235
 - SNMP-SERVER USER command 237, 239, 241
 - SNMPv1 and SNMPv2c
 - community names 60
 - described 59
 - setting 59
 - software configuration
 - adding a privilege level 31
 - adding a user and password 31
 - copying 39, 81, 86
 - displaying 38, 153
 - uploading 82, 84, 113
 - source ports in a port mirror 43
 - Spanning Tree Protocol (STP)
 - disabling 64
 - displaying 63
 - enabling 64
 - setting 62
 - setting priority 64
 - SHOW SPANNING-TREE command 106, 244
 - SPANNING-TREE ENABLE command 247
 - SPANNING-TREE FORWARD-TIME command 249
 - SPANNING-TREE HELLO-TIME command 250
 - SPANNING-TREE MAX-AGE command 251
 - SPANNING-TREE MODE command 252
 - SPANNING-TREE PORTFAST BPDU-FILTER command 253
 - SPANNING-TREE PORTFAST BPDU-GUARD command 254
 - SPANNING-TREE PRIORITY command 255
 - SPANNING-TREE ENABLE command 247
 - SPANNING-TREE FORWARD-TIME command 249
 - SPANNING-TREE HELLO-TIME command 250
 - SPANNING-TREE MAX-AGE command 251
 - SPANNING-TREE MODE command 252
 - SPANNING-TREE PORTFAST BPDU-FILTER command 253
 - SPANNING-TREE PORTFAST BPDU-GUARD command 254
 - SPANNING-TREE PRIORITY command 255
 - SPEED command 44, 182
 - SSH. See Secure Shell (SSH)
 - STATIC-CHANNEL-GROUP command 49, 184
 - STORM-CONTROL command 51, 185
 - switch
 - assigning an IP address 28
 - downloading software 35, 87
 - getting help 127
 - naming 128
 - rebooting 35
 - resetting to factory defaults 35
 - setting a gateway address 29
 - setting DHCP 29
 - setting jumbo frames 31
 - setting the network time 29
 - specifying a user name 31, 162
 - specifying passwords 31, 162
 - specifying the privilege level 31, 162
 - SWITCHPORT ACCESS VLAN command 41, 187
 - SWITCHPORT MODE TRUNK command 188
 - SWITCHPORT PORT-SECURITY MAXIMUM command 47, 48, 220, 222
 - SWITCHPORT PORT-SECURITY MODE command 48, 49, 223, 225
 - SWITCHPORT TRUNK ALLOWED VLAN command 42, 190, 265
 - SYSTEM FACTORY-RESET command 35, 111
 - SYSTEM REBOOT command 35, 112
- ## T
- Telnet
 - LINE VTY command 136
 - traffic 50
 - TRAFFIC-CLASS-TABLE USER-PRIORITY NUM-TRAFFIC-CLASSES command 192
 - trap receivers 61
- ## U
- upgrading software 35
 - UPLOAD command 113
 - USERNAME command 31, 162
 - USER-PRIORITY command 193
- ## V
- Virtual LAN. See VLAN
 - VLAN
 - adding tagged ports 42
 - adding untagged ports 41
 - changing the default 42, 187, 190, 265
 - creating 40, 41, 267
 - VLAN command 41, 267
 - VLAN DATABASE command 268, 269
 - VLAN mode
 - HELP command 127
 - SHOW RUNNING-CONFIG command 153
 - SHOW RUNNING-CONFIG FULL command 158